U.S. Department of Homeland Security
601 South 12th Street
Arlington, VA 20598

Transportation
Security
Administration

June 15, 2020

Henry Kerner
Special Counsel
U.S. Office of Special Counsel
1730 M Street, Suite 300
Washington, DC 20036-4505

RE: OSC File Nos. DI-18-5205 and DI-19-0778

Dear Mr. Kerner:

The attached report is in response to the December 18, 2018 referral of the above-captioned matters to the Secretary of the Department of Homeland Security (DHS) regarding a disclosure received by your office. The Secretary referred this inquiry to TSA for investigation. Consistent with delegations from the DHS Secretary and Undersecretary for Management, I am the designated official authorized to oversee the investigation and take any appropriate action determined to be necessary in accordance with 5 U.S.C. §1213(d). The Department's findings are included in the attached Report of Investigation (ROI). There does not appear to be any violation or apparent violation of any law, rule, or regulation.

Specifically, OSC characterized former Federal Air Marshal (FAM) Robert MacLean's disclosures as follows: 1) TSA's failure to properly protect flight crews and the public from potential opiod attacks; and 2) TSA's failure to prevent significant security breaches because of its policy exempting religious food trucks from airport inspections. More specifically, according to OSC, former FAM MacLean asserted that TSA is failing to secure aircraft from terrorist attacks using synthetic opioids and that he has not observed any changes in TSA protocol after reporting his concerns from February through September 2018. Further, former FAM MacLean asserted that exempting religious food trucks from airport inspections represents a threat to aviation security. The investigation revealed that TSA did not engage in a failure to protect flight crews and the public or a failure to prevent significant security breaches. Rather, TSA has addressed and continues to address each of these issues.

Regarding potential fentanyl exposure on an aircraft, screening procedures are designed to prevent unknown powders from being brought aboard aircraft. Transportation Security Officers (TSOs) screen accessible property for powders at the screening checkpoint. In May 2018, TSA implemented Enhanced Accessible Property Screening (EAPS) which provides for screening both organic powder-like material and inorganic powder-like material and increased the search rates of powders. Specific procedures for screening powders include visual and physical inspections, explosive trace detection searches and colorimetric testing. Regarding exposure at the screening checkpoint, TSA also made numerous safety and procedural changes. TSA equipped TSOs with thicker gloves (5mil Nitrile), provided awareness briefings, and established employee handling and response procedures. If a TSO finds a powder that could be fentanyl, the TSO should not open the container or conduct additional screening of the powder. The TSO should notify a supervisor who will notify law enforcement.

Additionally, in September 2017, TSA requested that the National Institute for Occupational Safety and Health (NIOSH) perform a health hazard evaluation regarding potential exposure to fentanyl among TSA employees. NIOSH recommendations included continuing safety practices in standard operating procedures, providing training, and continuing the use of 5 mil nitrile gloves. TSA is in compliance with implementing the recommended safety protocols. For workforce protection, TSA has also provided awareness briefings and training to the Law Enforcement/Federal Air Marshal Service (LE/FAMS) workforce and held working group meetings of FAMs to discuss these issues. Lastly, TSA has found no indication that terrorist or criminal adversaries intend to release fentanyl in the civil aviation sector.

These issues regarding fentanyl in the transportation domain continue to be monitored. Despite the lack of intelligence reporting indicating that terrorist or criminal adversaries intend to release fentanyl in the civil aviation sector, TSA submitted this issue into its Security Vulnerability Management Process for evaluation to formally assess the risk. In the future, should it be determined that a threat of fentanyl bypassing the screening checkpoint requires agency action, TSA would consider options broader than remedies available only to FAM-covered flights.

Regarding the second issue, TSA has found no intelligence supporting the idea that terrorists are considering food trucks as a method of attack. As there is an insider threat risk throughout the transportation sector, TSA has a layered security approach to secure catering trucks. First, there is no difference in requirements for "religious food trucks" vis-à-vis any other catering truck. Security requirements are implemented throughout the process, beginning at the catering facility when catering carts are visually inspected and there is a random pull of food trays to examine for signs of tampering. Catering trucks must either be sealed or escorted/monitored from the time they leave the catering facility and the seal cannot be broken except by the aircraft operator or an authorized representative.

The Compliance Division in Security Operations is responsible for inspecting regulated entities to ensure all security requirements are followed. As catering operations are identified as "High Risk" on the Compliance Risk Register, these operations are consistenly subjected to inspections, testing and oversight. These inspections include comprehensive inspections of the air carrier covering all regulated areas, targeted inspections, supplemental inspections, or Special Emphasis Assessments or Special Emphasis Inspections that are scheduled as needed. Inspectors also perform covert testing, such as testing to ensure that appropriate procedures are followed if there is a broken security seal.

As TSA recognizes that the insider threat risk exists in the catering operation as it does throughout the transportation system, there are also requirements that must be met for the individuals performing the catering security functions. First, the employees of the catering companies do not perform security measures; these are performed by a designated aircraft operator employee or an authorized representative who is not employed by a catering company. Additionally, the domestic air carrier security program requires that individuals performing the catering security functions have an airport-issued or approved identification media, which would subject them to a fingerprint-based criminal history records check and a security threat assessment. For foreign air carriers, TSA requires an airport-issued identification for individuals performing catering security functions. If there is not such identification, the person must have provided 10 years of employment history and the foreign air carrier must verify the most recent five years of employment.

More recently, in October 2018, the TSA Administrator sought assistance from an industry advisory group, the Aviation Security Advisory Committee (ASAC) on insider threat issues. The ASAC Insider Threat Subcommittee focused on a detailed review of the work of the internal TSA Insider Threat Advisory Group and made recommendations. If implemented, some of the recommendations may impact individuals working in catering facilities and catering security controls. TSA will consider these recommendations and continue to collaborate with ASAC on these issues.

If you require further information regarding this matter, please do not hesitate to contact [redacted] [redacted] Assistant Chief Counsel, at [redacted]

Sincerely yours,

Patricia F.S. Cogswell

Patricia F.S. Cogswell
Acting Deputy Administrator
Transportation Security Administration

Attachment

cc: [redacted]
Executive Assistant Administrator
Law Enforcement/Federal Air Marshal Service

[redacted]
Director, Enterprise Performance & Risk
Strategy, Policy Coordination, and Innovation

Department of Homeland Security
Transportation Security Administration
Report of Investigation

CASE NUMBER: I19 0050 **PR CASE:** NO

TITLE: Office of Special Counsel Disclosures (DI-18-5205 and DI-19-0778)

CROSS REFERENCED CASES: N/A

SUBJECT(S):

Name: Transportation Security Administration
Duty title: N/A
Pay band: N/A
Duty location: N/A
EOD: N/A
Administrative Status: N/A

ALLEGATION(S):

5 U.S.C. 1213

- TSA has failed to properly protect flight crews and the public from potential opioid attacks; and
- TSA has failed to prevent significant security breaches because of its policy exempting religious food trucks from airport inspections.

PERIOD OF INVESTIGATION:

February 12, 2019 – June 17, 2019

CASE STATUS: Closed

INVESTIGATED BY: Transportation Security Specialists "A" & "B," Investigator "C," and Special Agents [redacted] and [redacted]

REPORT BY: Transportation Security Specialist "A"

[redacted]

[redacted]
Special Agent in Charge
Headquarters Operations Branch
TSA Investigations

February 6, 2020
Date

REPORT DISTRIBUTION

☐ Assistant Administrator, Professional Responsibility

☒ Chief Counsel

☐ Assistant Administrator/Director, Federal Air Marshal Service

☐ Assistant Administrator, Security Operations

☐ Federal Security Director - ______________________________

☒ Other–Office of Special Counsel and TSA Enterprise Performance and Risk

☒ File

Report of Investigation (ROI) Handling: The ROI and information contained herein are subject to the Privacy Act of 1974 (5 U.S.C. 552A, Public Law 93-579) and thus may not be released outside official channels. This material must be safeguarded from unauthorized disclosure, and should not be left unattended or discussed with unauthorized persons, and must be retained in a security container when not in use.

This report or any portion thereof may not be released to the subject of the investigation or any individual identified therein, or their representatives, or reproduced without the written consent of TSA Investigations.

Origin of Case:

On February 11, 2019, TSA Investigations (INV) was notified by TSA Chief Counsel that Office of Special Counsel (OSC) whistleblower disclosures (OSC File No. DI-18-5205 and DI-19-0778) alleged the following:

- TSA has failed to properly protect flight crews and the public from potential opioid attacks; and
- TSA has failed to prevent significant security breaches because of its policy exempting religious food trucks from airport inspections.

The disclosure was made by former TSA Federal Air Marshal (FAM) Robert MacLean[1]

Executive Summary

Information with respect to which the Investigation was Initiated

On February 11, 2019, INV was notified, by TSA Chief Counsel, that OSC whistleblower disclosures (OSC File No. DI-18-5205 and DI-19-0778) alleged the following:

- TSA has failed to properly protect flight crews and the public from potential opioid attacks; and
- TSA has failed to prevent significant security breaches because of its policy exempting religious food trucks from airport inspections.

The disclosure was made by former TSA FAM Robert MacLean.

Conduct of Investigation

INV interviewed and collected statements from FAM MacLean, representatives from Chief Counsel, Law Enforcement/FAMS, Enterprise Performance and Risk, Human Capital, Intelligence and Analysis, the Occupational Safety, Health and Environment (OSHE) Division, and Security Operations.

Summary of Evidence

The investigative activities revealed that TSA:

- Is aware of the issues surrounding Fentanyl as a potential threat and has found no indication that terrorist or criminal adversaries intend to release Fentanyl in the civil aviation sector.
- Has provided awareness briefs and training to the LE/FAMS workforce on the dangers of Fentanyl and continue to monitor the issue from a workforce protection perspective but, as of this writing, have not made any operational changes to address a Fentanyl exposure onboard an aircraft.
- Has made numerous safety and procedural changes to protect both the public and workforce from Fentanyl exposure at the security screening checkpoints;

[1] During the course of this investigation, Robert MacLean was terminated from TSA.

- Is in compliance with relevant safety protocols recommended by TSA's Occupational Safety, Health, & Environment (OSHE) Division;
- Does not have a policy, nor, is there a Federal regulation exempting religious food trucks or any food trucks from inspection. TSA has a layered approach to secure catering trucks and all are subject to the same security requirements regardless of the food inside. This layered approach includes inspections, testing and oversight as well as requirements that must be met for individuals performing the catering security functions;
- Is considering recommendations made by the Aviation Security Advisory Committee regarding insider threat issues, some of which may impact catering facilities and individuals working in catering facilities;
- Found no intelligence to support the idea that terrorists have considered or are considering opioids or food trucks as a method of attack; and
- Is positioned to formally assess the risk that Fentanyl and/or an airport catering operation poses as it subscribes to enterprise risk management and has an established risk assessment process that allows TSA to make decisions and respond to opportunities and risks as they arise.

Violations or Apparent Violations of any Law, Rule, or Regulation

INV found no violation or apparent violation of any law, rule, or regulation.

Agency Action Taken or Planned as a Result of the Investigation

This report is being submitted into TSA's Security Vulnerability Management Process, in the TSA Enterprise Performance and Risk office, for evaluation and consideration of the risk of Fentanyl being released in the civil aviation sector.

There is no additional agency action planned regarding catering trucks as a result of the investigation. TSA will continue its layered security approach and consider the May 2019 Aviation Security Advisory Committee's recommendations.

Allegation #1:

TSA has failed to properly protect flight crews and the public from potential opioid attacks.

Finding #1:

During MacLean's testimony, he explained to INV that his concern was related specifically to the opioid Fentanyl. The investigative activities revealed that:

- According to Law Enforcement/Federal Air Marshal Service (LE/FAMS) Director, [redacted] TSA Chief Medical Officer (CMO), [redacted] Enterprise Performance and Risk Director (EP&R), [redacted] Security Operations Transportation Security Specialist (TSS), [redacted] and Intelligence and Analysis (I&A) Senior Analyst "D," TSA (the agency) is aware of the issues surrounding Fentanyl as a potential threat. TSA has found no indication that terrorist or criminal adversaries intend to release Fentanyl in the civil aviation sector. However, the agency acknowledged that it cannot rule out the intentional release of it by a terrorist, as the lethality of exposure to it is publicly available;
- On February 8, 2019, [redacted] LE/FAMS Director of Field Operations, was interviewed and stated that the TSA LE/FAMS has provided awareness briefs and training to the FAM workforce on the dangers of Fentanyl and continue to monitor the issue from a workforce protection perspective but, as of this writing, have not made any operational changes to address a Fentanyl exposure onboard an aircraft;
- On March 6 and 11, 2019, Security Operations TSS [redacted] and Dr. [redacted] CMO were interviewed and stated that TSA has made numerous changes to safety and emergency response protocols, to protect both the public and workforce from Fentanyl exposure, at the security screening checkpoints; and
- On March 26, 2019, EP&R Director, [redacted] was interviewed and stated that TSA is positioned to more formally assess the risk that Fentanyl poses as it subscribes to enterprise risk management and has an established risk assessment process. This process establishes the context for risks, as well as identifies analyzes, evaluates, responds to, monitors, and communicates them in a way that allows TSA to make decisions and sensibly respond to opportunities and risk as they arise.

Discussion:

Threat Scenario, Recommendations and Impact of Fentanyl Exposure

Former FAM MacLean testified that his concern with Fentanyl was related to a FAM being unprepared to mitigate a flight crew's exposure to the opioid if it was thrown into the cockpit by a person wanting to gain control of the aircraft as Fentanyl is easily accessible, highly profitable, compact, transports easily, and lethal even in small quantities.

MacLean recommends that TSA equip the FAMs with the Fentanyl antidote Naloxone HCl (NARCAN) in addition to making changes related to flight deck operations. These include:

- Requiring aircraft be equipped with secondary barrier seals for the forward galley that are bullet proof, and powder proof;
- Requiring that the cockpit be equipped with NARCAN;
- Eliminating the operation of the seat belt sign as a pre-cursor to the pilot leaving the cockpit;
- Eliminating the notification process when the pilot is planning on leaving the cockpit;
- Equipping a motion sensor in the aircraft lavatory; and
- Equipping the cockpit with a key, accessible only to the pilot/co-pilot that unlocks the flight deck door.

Fentanyl is approximately 50-100x more powerful than Morphine and Carfentanil (Fentanyl analog) is approximately 10x more powerful than Fentanyl. The United States Department of Defense has been researching Fentanyl as a weapon for over 20 years and numerous studies have been conducted onboard aircraft. Fentanyl was first seen discussed, as a potential threat, in open source forums in 2005.

Fentanyl can enter the blood stream intravenously, via inhalation, pill, or through dermal means. Inhalation of Fentanyl is the most dangerous method of consumption, the peak narcotic response for this method is minutes. Dermal contact has a much longer peak narcotic response time of 20-72 hours.

According to former Department of Defense Research Chemist, Dr. Christina Baxter and Don Ostrowski of Federal Resources, if a localized Fentanyl release is done on an aircraft, the persons closest to the release would be affected. However, the ventilation system on most aircraft includes filters that would collect the Fentanyl particulates reducing the possibility of recirculation. If this were to occur, it is recommended that the flight crew use supplied air as soon as possible. The treatment for a Fentanyl overdose is NARCAN and can be used when the victim displays respiratory distress. It takes approximately 2-3 minutes to work.

Open source reporting shows more interest in using other agents as weapons such as Hydrogen Cyanide, Hydrogen Sulfide, Phosphine, Arsine, and Phosgene.

Threat Intelligence and Enterprise Risk

TSA is an intelligence driven, risk-based agency as it must carry out its mission to "protect the Nation's transportation systems to ensure freedom of movement for people and commerce" within various resource constraints. It must face the persistent challenge of outmatching a committed and adaptive adversary and, as such, have the most effective security in the most efficient way.

TSA Intelligence and Analysis (I&A) wrote an unclassified intelligence assessment titled "Threat of Fatal Contact with Fentanyl," dated November 20, 2017 that stated, "We have no indications terrorist or criminal adversaries intend to release Fentanyl in the civil aviation sector. Fentanyl can be and likely has been weaponized as a liquid aerosol by foreign governments; however, we cannot rule out the accidental release of Fentanyl within an aircraft or checkpoint, or terrorist intentional use of it, as the lethality of exposure to Fentanyl is publicly available and in the open source media".

The Department of Homeland Security defines "risk" as the "potential for an unwanted outcome as determined by its likelihood and the consequences."[2] To address risk, TSA subscribes to enterprise risk management (ERM). ERM enables TSA to more effectively manage enterprise level risks, and it enables agency leaders to consider the trade-offs between risks, associated costs, and value creation across the organization. It provides a logical and systematic method for establishing the context for risks, as well as identifying, analyzing, evaluating, responding to, monitoring, and communicating them in a way that allows TSA to make decisions and sensibly respond to opportunities and risk as they arise.

TSA's EP&R office conducts formal risk assessments based on direction from TSA senior leadership, intelligence information, and/or a request from a program office or employee. They maintain an Enterprise Risk Register (ERR) that currently outlines 17 risks that have been formally assessed and categorized based on TSA's risk appetite (Risk Averse, Risk Neutral and Risk Tolerant). EP&R has not conducted, nor, has been requested to conduct a risk assessment of a Fentanyl/opioid attack on board an aircraft, however the agency has the processes in place to do so if the need arises.

Risk Mitigation Efforts

Despite the fact that there is currently no threat intelligence indicating the use of Fentanyl in the civil aviation sector and a formal risk assessment has not been conducted on the issue, TSA's LE/FAMS has been looking at this issue from a workforce protection perspective. The LE/FAMS have provided awareness briefs and training to the FAM workforce on the dangers of Fentanyl. The LE/FAMS Medical Programs wrote an issue paper titled "Fentanyl, Increasing Workforce Protection" dated April 2018 and held a working group to review and discuss increasing the protective posture for operational FAMs. The discussions included trying to identify the purpose of issuing NARCAN and associated legal issues, such as whether it would be issued solely for the personal protection of a FAM or used to assist others (flight crew/passenger) on the aircraft. As of this writing, LE/FAMS continue to monitor the threat and explore options to protect personnel. This effort is ongoing.

Additionally, in September 2017, the TSA Director of the Occupational Safety, Health and Environment (OSHE) Division, [redacted] requested a health hazard evaluation (HHE) be conducted, by the National Institute for Occupational Safety and Health (NIOSH), on the potential exposure to fentanyl and fentanyl analogs among TSA employees during security screening operations and other selected activities at airports nationwide. NIOSH concluded that the "safety and health program for TSA Security Officers includes appropriate training, standard operating procedures for work practices, and PPE requirements." NIOSH did not recommend anything additional for TSA to implement.

[2] DHS Lexicon issued May 26, 2017

NIOSH did not review the specific work activities and duties of FAMs as part of the HHE. However, they did note that a number of recommendations in the report would apply to FAMs.

In May 2018, TSA implemented the Enhanced Accessible Property Screening (EAPS) procedures which added a requirement to screen organic powder in addition to already screening inorganic powder. With the addition of screening organic powders and the increasing illicit use of Fentanyl, TSA predicted that the chances of the TSA screening workforce coming into contact with it would increase. As a result, TSA took numerous steps, in accordance with recommendations from OSHE and concurred with by NIOSH, to protect the workforce from Fentanyl exposure. These steps included equipping Transportation Security Officers (TSOs) with thicker gloves (5mm Nitrile), providing awareness briefs about the narcotic and establishing employee handling and response procedures.

According to Director [redacted] TSA is compliant with the safety protocols implemented to mitigate the risk of an employee's potential exposure to Fentanyl and/or a Fentanyl analog.

Allegation #2:

TSA has failed to prevent significant security breaches because of its policy exempting religious food trucks from airport inspections.

Finding #2:

INV's investigative activities revealed that:

- According to Security Operations Regional Security Inspector [redacted] Transportation Security Inspector "E," Section Chief [redacted] I&A Senior Intelligence Analyst "D," and LE/FAMS Supervisory Air Marshal in Charge, [redacted] TSA does not have a policy nor is there a Federal regulation exempting religious food trucks or any food trucks from inspection. TSA has a layered approach to secure catering trucks and all are subject to the same security requirements regardless of the food inside. An airport catering operation is a potential insider threat risk to transportation security, however, TSA found no intelligence to support the idea that terrorists have considered or are considering food trucks as a method of attack.

Discussion:

During MacLean's testimony, he stated that his lack of authority as a FAM to conduct a random search ("break the seal and open") of a catering truck during a Visible Intermodal Prevention and Response (VIPR) operation, created an "insider threat" vulnerability. He explained that these trucks could be carrying contraband since from the time they leave the catering facility until they get to the aircraft, they are not subject to search. He proposed that TSA convey search authority to the agency's law enforcement personnel to conduct random searches of these vehicles.

Federal Regulations and TSA Policies

Aircraft Operators (domestic and foreign) and/or their authorized representative are the regulated entities that are responsible for following federal regulations and policies related to airport catering operations. TSA Security Operations, Compliance Division is delegated the responsibility for inspecting these regulated entities and their authorized representatives to ensure all applicable Federal regulations and security requirements are followed.

The regulations/policies that outline how aircraft operators must secure the catering for their flights are as follows:

- Code of Federal Regulations (CFRs) – 49 CFR §1540, §1544 and §1546;
- Aircraft Operator Standard Security Program (AOSSP) Chapter 10 for domestic air carriers; and
- Emergency Amendment (EA) 1546-12-07L for foreign air carriers.

These regulations/policies include requirements for securing the catering carts when it is being "made up" at the catering facility and when the catering is being transported to the aircraft. All catering carts and catering supplies are visually inspected by the aircraft operator (or authorized representative) to look for items that don't belong. The visual inspection is limited by local laws and hygiene standards. After the visual inspection, the air carrier must randomly pull food trays to look for signs of tampering.

Additionally, catering trucks are subject to a robust security and screening program that includes rules regarding sealing, monitoring, inspecting and testing.

Regarding the catering security personnel, the domestic air carrier security program (AOSSP Chapter 10) requires that individuals performing the catering security functions required by the program, have an airport-issued or approved identification media, which would subject them to a fingerprint-based criminal history records check (CHRC) and a security threat assessment (STA)[3]. For foreign air carriers, TSA requires the catering security personnel either have an airport-issued identification (and the required CHRC and STA) or they must have the employee provide 10 years of employment history and the foreign air carrier must verify the most recent 5 years of employment. There is no TSA requirement for the catering personnel to have a background check.

TSA's Security Operations Compliance Division is responsible for ensuring regulated entities are complying with Federal regulations and agency policies. They utilize numerous tools such as intelligence, compliance data, the TSA "Compliance Risk Register" (CRR), and other risk-based factors to drive compliance efforts across the Nation.

The CRR is a "strategic assessment of regulatory security requirements and is one of the foundations of TSA's regulatory compliance operations" and "enables TSA and regulated parties to improve risk-based decision making and implement mitigation activities across the Nation's transportation system." It was developed by analyzing "security risks employing a rigorous methodology that evaluates the potential impact resulting from the failure of regulated entities to effectively comply with transportation security requirements."

[3] An STA consists of a background check against Federally maintained databases to establish any link to terrorism. Persons required to undergo an STA include but are not limited to: persons obtaining an Airport issued ID granting access to the Secure Area, Indirect Air Carrier employees and owners, persons with unescorted access to cargo.

The CRR also enables the Compliance Division to analyze data, identify, and report on compliance trends. Compliance trends along with intelligence and other risk-based factors drive informed decisions regarding the implementation of compliance operations that can focus on overall operations or specific areas such as catering. Such operations include Special Emphasis Assessments (SEA), Compliance Security Enhancement Through Testing (COMSETT), Special Emphasis Inspections (SEI), Comprehensive and/or Supplemental inspections, and outreaches that are conducted by TSA Transportation Security Inspectors (TSIs) throughout the enterprise. Catering operations are identified on the CRR, within the Compliance Division's area of responsibility, and are subject to a rigorous inspection and testing program.

Insider Threat and Enterprise Risk

TSA defines "Insider Threat" as "one or more individuals with access and/or insider knowledge that allows them to exploit vulnerabilities of the Nation's transportation systems with the intent to cause harm."

During this investigation, INV conducted field observations of both on and off airport catering facilities, and discussed catering security with TSA compliance personnel. The "Insider Threat" was noted as the biggest vulnerability within the catering operation.

The process most susceptible to insider threat would be when the carts are being assembled as the last person to have access to a catering cart is a catering security officer as he/she searches it then closes and seals the cart prior to it being loaded on the truck, transported to the airport and loaded on an aircraft.

It must be noted that the "insider threat" risk exists across the transportation system, not just within the catering operation. There are thousands of "insiders", government and private employees that work within the transportation security domain.

TSA has identified the insider threat as high risk as it exists across the transportation security enterprise. TSA's Enterprise Performance and Risk program, which focuses on risks that impact the entire agency, has not specifically assessed the risk of airport catering security operations/protocols.

Thus, the agency is positioned to formally assess the risk of a specific threat within the insider threat arena (e.g. catering operation) as their process establishes the context for risks, as well as identifies analyzes, evaluates, responds to, monitors, and communicates them in a way that allows TSA to make decisions and sensibly respond to opportunities and risk as they arise.

TSA has an Insider Threat Program governed by TSA Management Directive 2800.17 and led by LE/FAMS. The Insider Threat Unit continually monitors and reviews insider threats, handles insider threat and/or investigative referrals, and leads the Insider Threat Advisory Group.

The Aviation Security Advisory Committee's Insider Threat Subcommittee recently focused on a detailed review of the work of the Insider Threat Advisory Group and submitted recommendations to TSA. TSA is considering these recommendations, some of which may impact catering operations.

TSA's Insider Threat Advisory Group developed an Insider Threat Response Plan that describes lines of effort and specific activities that TSA is conducting to counter insider threat. The group identified, ranked and prioritized the challenges in these areas based on risk and return on investment. The rankings are as follows: First Priority, Second Priority, Third Priority, and Risk Mitigated based on the risk posed to the transportation sector and the likely cost to mitigate the risk.

The scenario of secreting a device on a catering tray (which would be transported in catering vehicle) and the personnel vetting were both ranked as a second priority. The vulnerabilities that are ranked higher are considered more impactful and more likely to be exploited thus those are the areas where the Insider Threat Program efforts are focused.

> **Note:** Not all catering employees undergo a CHRC, however all employees who conduct the catering security requirements are required to have a fingerprint based CHRC.

As the insider threat exists across the enterprise, TSA also has other offices that monitor and review the threat and risks posed by insiders such as EP&R, I&A and Security Operations. The agency implements numerous mitigation strategies including but not limited to, aviation worker vetting, intelligence analysis, joint vulnerability assessments, compliance inspections, random screening, red team testing, and network defense that are applied across the entire transportation security enterprise.

OTHER INVESTIGATIVE ASPECTS

Persons Associated with Case:

Name	Role	Title
[redacted]	Witness	Trans. Sec. Inspector
[redacted]	Witness	Director
[redacted]	Witness	Section Chief
[redacted]	Witness	Trans. Security Spec.
[redacted]	Witness	Chief Medical Officer
MacLean, Robert	Whistleblower	Former FAM
[redacted]	Witness	Operations Research Analyst
[redacted]	Witness	Director, Field Ops, FAMS
[redacted]	Witness	Supervisory FAM
[redacted]	Witness	Senior Intelligence Analyst
[redacted]	Witness	Attorney/Advisor
[redacted]	Witness	Supv. FAM in Charge
[redacted]	Witness	Asst. Supv. FAM in Charge
[redacted]	Witness	Director, OSHE
[redacted]	Witness	Regional Security Inspector

April 26, 2021

OSC Matters: DI-18-5205 and DI-19-0778
TSA Supplemental Information Provided in Response to OSC Questions

1. **The report states that specific procedures for screening powders include visual and physical inspections, explosive trace detection services, and colorimetric testing. (*See* bottom of page 1/Top of page 2).**
   a. **Please explain in detail what these procedures entail.**

These procedural details are in screening Standard Operating Procedures and are unable to be provided without including Sensitive Security Information (SSI).

Note that TSA's screening procedures are focused on security and are designed to detect potential threats to aviation and passengers. Accordingly, TSA security officers do not search for illegal drugs, but if any illegal substance is discovered during security screening, TSA will refer the matter to a law enforcement officer.

   b. **What is the smallest amount of powder that can be detected?**

For ETDs, the amounts needed are classified at the Secret level. The unclassified non-SSI answer is a fingerprint; the amount is not visible to the Human Eye. For colorimetric testing, a few visible grains are needed on the swab. The swab is "sticky" so it will pick up and hold onto the grains.

2. **The report states that "accessible property" is searched. (*See* page 1, para. 3)**
   a. **What does DHS consider to be accessible property?**

Accessible property is property that is intended to be available to the individual in the sterile area or in the cabin of the aircraft. For example, see references to accessible property on the following websites:
Disabilities and Medical Conditions | Transportation Security Administration (tsa.gov)
Traveling with Children | Transportation Security Administration (tsa.gov)

3. **OSC's understanding is that in June 2018, TSA announced that it would screen powder-like substances greater than 12oz/350ml, about the size of a soda can, from carry-on luggage.**
   a. **Is this true?**

Powders of that size may receive additional screening. See the following link with respect to baby powder, for example:
What Can I Bring? | Transportation Security Administration (tsa.gov)
The website states:

> Powder-like substances greater than 12 oz. / 350 mL must be placed in a separate bin for X-ray screening. They may require additional screening and containers may need to be

> opened. For your convenience, we encourage you to place non-essential powders greater than 12 oz. in checked bags.

Please also see the following link:
What is the policy on powders? Are they allowed? | Transportation Security Administration (tsa.gov)
The website states:

> Starting June 30, 2018, if you are traveling from an international last-point-of-departure to the U.S., powder-based substances in carry-on baggage greater than 350mL or 12 oz. may require additional screening at the central checkpoint. Powder-like substances over 12 oz. or 350mL in carry-on that cannot be resolved at the central checkpoint will not be allowed onto the cabin of the aircraft and will be disposed of.
>
> For your convenience, place powders in your checked bag.
>
> The measures have already been implemented at U.S. airports nationwide to identify and prevent potentially dangerous items from being brought aboard the aircraft. There are no changes to what is allowed in carry-on baggage at U.S. airport checkpoints.

b. **How much powder triggers a search?**

Powder-like substances greater than 12oz/350ml, about the size of a soda can, may require additional screening.

4. **The report states that regarding exposure at the screening checkpoint, TSA also made numerous procedural and structural changes. (*See* page 2, top of page.)**

a. **On what dates did these changes occur?**

TSA approved equipping TSOs with thicker 5 mil nitrile gloves on June 13, 2017.
National Shift Briefs issued on June 3, 2017, February 24, 2018, July 11, 2018, October 31, 2018, and November 2, 2018 provided information regarding Fentanyl.

5. **What measures have DHS put in place to protect flight crews and the public from potential opioid exposure?**

Regarding potential fentanyl exposure on an aircraft, screening procedures are designed to prevent unknown powders from being brought aboard aircraft. Transportation Security Officers (TSOs) screen accessible property for powders at the screening checkpoint. In May 2018, TSA implemented Enhanced Accessible Property Screening (EAPS) which provides for screening both organic powder-like material and inorganic powder-like material and increased the search rates of powders. Specific procedures for screening powders include visual and physical inspections, explosive trace detection searches and colorimetric testing. Regarding exposure at the screening checkpoint, TSA also made numerous safety and procedural changes. TSA equipped TSOs with thicker gloves (5mil Nitrile), provided awareness briefings, and established employee handling and response procedures. If a TSO finds a powder that could be fentanyl, the

TSO should not open the container or conduct additional screening of the powder. The TSO should notify a supervisor who will notify law enforcement.

Additionally, in September 2017, TSA requested that the National Institute for Occupational Safety and Health (NIOSH) perform a health hazard evaluation regarding potential exposure to fentanyl among TSA employees. NIOSH recommendations included continuing safety practices in standard operating procedures, providing training, and continuing the use of 5 mil nitrile gloves. TSA is in compliance with implementing the recommended safety protocols. For workforce protection, TSA has also provided awareness briefings and training to the Law Enforcement/Federal Air Marshal Service (LE/FAMS) workforce and held working group meetings of FAMs to discuss these issues. Lastly, TSA has found no indication that terrorist or criminal adversaries intend to release fentanyl in the civil aviation sector.

These issues regarding fentanyl in the transportation domain continue to be monitored. Despite the lack of intelligence reporting indicating that terrorist or criminal adversaries intend to release fentanyl in the civil aviation sector, TSA submitted this issue into its Security Vulnerability Management Process for evaluation to formally assess the risk. This assessment was presented to the TSA Executive Risk Steering Committee in February 2020.

6. **Will DHS require aircraft operators to carry Narcan, which counteracts opioid exposure, in the event of an emergency? If not, please explain.**

This issue falls within the Federal Aviation Administration's (FAA) responsibilities. See FAA regulations, 14 C.F.R. § 121.803 and Appendix A to Part 121, for information regarding First Aid Kits and Emergency Medical Kits. See also FAA Advisory Circular 121-33B, *Emergency Medical Equipment*.

7. **Are flight crews required to be trained in recognizing opioid exposure and administering Narcan? If not, please explain.**

The FAA, not the TSA, is responsible for the training requirements for flight crew. See FAA regulations, 14 C.F.R. § 121.805, regarding crewmember training for in-flight medical events. See also FAA Advisory Circular 121-34B, *Emergency Medical Equipment Training*.

Advisory Circular

Subject: EMERGENCY MEDICAL EQUIPMENT

Date: 1/12/06

Initiated by: AFS-220
AAM-210

AC No: 121-33B

1. What is the purpose of this advisory circular (AC)?

This AC provides guidance about onboard emergency medical equipment, including Automated External Defibrillators (AED) and Emergency Medical Kits (EMK). It is intended to guide air carriers when establishing protocols for emergency medical equipment. The Federal Aviation Administration (FAA) expects and anticipates some variation among the programs that air carriers establish for emergency medical equipment. (Also see AC 121-34B, Emergency Medical Equipment Training.)

2. Does this AC supersede any existing ACs?

This AC supersedes AC 121-33A, Emergency Medical Equipment, dated May 9, 2003. It also relates to existing AC 120-44A, Air Carrier First Aid Programs (http://www.faa.gov/avr/afs/cabinsafety/acidx.cfm), which is also a good reference source.

3. What FAA regulations does this AC cover?

Title 14 of the Code of Federal Regulations (14 CFR) part 121, subpart X; part 121, appendix A. (http://www.gpoaccess.gov/ecfr).

4. Who should read this AC?

FAA aviation safety inspectors (cabin safety and operations), part 121 air carrier certificate holders, directors of operations, directors of safety, crewmembers, AED manufacturers and suppliers, EMK suppliers, as well as people involved in the development of air carrier procedures and training programs. This AC may also be valuable to people associated with operations under 14 CFR part 125, part 135, and subpart K of part 91 (fractional ownership programs).

5. When is an emergency medical kit and an AED required and on what size of aircraft?

The FAA requires AEDs on all airplanes of air carriers operating under part 121 with a maximum payload capacity of more than 7,500 pounds and with at least one flight attendant. Affected airplanes typically would have a capacity for 30 passengers or more requiring at least one flight attendant. The FAA also requires an EMK on all airplanes of air carriers operating under part 121 for which at least one flight attendant is required. EMKs and AEDs are “no-go” items and must be carried as indicated on the Minimum Equipment List.

6. What emergency medical equipment must air carriers carry?

At least one approved AED, legally marketed in the United States in accordance with Food and Drug Administration (FDA) requirements.

At least one approved EMK with the following items.

Part 121, appendix A, specifies that the following items must be carried in EMKs:

CONTENTS	QUANTITY
Sphygmomanometer	1
Stethoscope	1
Airways, oropharyngeal (3 sizes): 1 pediatric, 1 small adult, 1 large adult or equivalent	3
Self-inflating manual resuscitation device with 3 masks (1 pediatric, 1 small adult, 1 large adult or equivalent)	1: 3 masks
CPR mask (3 sizes), 1 pediatric, 1 small adult, 1 large adult, or equivalent	3
IV Admin Set: Tubing w/ 2 Y connectors	1
Alcohol sponges	2
Adhesive tape, 1-inch standard roll adhesive	1
Tape scissors	1 pair
Tourniquet	1
Saline solution, 500 cc	1
Protective nonpermeable gloves or equivalent[1]	1 pair
Needles (2-18 ga., 2-20 ga., 2-22 ga., or sizes necessary to administer required medications)	6
Syringes (1-5 cc, 2-10 cc, or sizes necessary to administer required medications)	4
Analgesic, non-narcotic, tablets, 325 mg	4
Antihistamine tablets, 25 mg	4
Antihistamine injectable, 50 mg, (single dose ampule or equivalent)	2
Atropine, 0.5 mg, 5 cc (single dose ampule or equivalent)	2
Aspirin tablets, 325 mg	4
Bronchodilator, inhaled (metered dose inhaler or equivalent)	1
Dextrose, 50%/50 cc injectable, (single dose ampule or equivalent)	1
Epinephrine 1:1000, 1 cc, injectable, (single dose ampule or equivalent)	2
Epinephrine 1:10,000, 2 cc, injectable, (single dose ampule or equivalent)	2
Lidocaine, 5 cc, 20 mg/ml, injectable (single dose ampule or equivalent)	2
Nitroglycerine tablets, 0.4 mg	10
Basic instructions for use of the drugs in the kit	1

[1] Although the FAA requires only one pair of protective gloves, it recommends that operators keep additional pairs accessible on the aircraft. This would allow crewmembers to access a pair of gloves without having to locate and open an EMK.

7. What is the purpose of the following items contained in the EMK?

- *Non-narcotic analgesic tablets:* a general oral medication used mainly to relieve muscle aches and headaches
- *Oral antihistamine:* medication used mainly to relieve symptoms associated with allergies and hay fever
- *Aspirin*: a general oral medication used mainly to alleviate head and muscle aches and chest pain or heart attack
- *Atropine:* medication used mainly to increase heart rate, that may be needed to assist a passenger with an unstable cardiac rhythm
- *Bronchodilator inhaler:* a preparation of medication used to help restore normal breathing in asthmatics
- *Epinephrine 1:10,000:* medication used mainly for cardiac resuscitation
- *Lidocaine:* medication used mainly in cases of unresponsiveness to defibrillation and possibly for maintenance of normal heart rhythm after successful defibrillation
- *An IV administration set including tubing with 2Y connectors (and, for placing the IV, alcohol sponges, tape, bandage scissors, and a tourniquet)*: equipment used for administering IV drugs (e.g., atropine, lidocaine, epinephrine) that may be needed to sustain heart function
- *A self-inflating manual resuscitation bag (AMBU bag) (with 3 masks: 1 pediatric, 1 small adult, and 1 large adult)*: equipment that may be needed for continuation of respiratory support
- *CPR mask (1 pediatric, 1 small adult, 1 large adult)*: equipment that may be needed to protect a person while administering CPR

8. What does "or equivalent" mean?

The FAA recommends that air carriers carry the required EMK items without substitution. The FAA has used the words "or equivalent" in part 121, appendix A, since 1986 (and will continue to use the words) to allow for any nomenclature or other changes the medical community might choose to make over the course of the lifetime of the regulation. The FAA references only generic terms under part 121, appendix A as amended. If you have a question about whether a certain medication or piece of equipment you choose to stock will meet the requirement, please contact the FAA Office of Aerospace Medicine.

Suppliers have asked the FAA whether diphenhydramine HCl injection is an acceptable equivalent to meet the requirement for antihistamine injectable. It is acceptable. They also have asked whether it is acceptable to stock universal masks where CPR masks or masks for resuscitation are required. In both situations, universal masks designed for the required sizes are acceptable as long as they meet the quantity requirements. In addition, some masks may be used to administer CPR and also may be used with the self-inflating manual resuscitation device. These masks often use a one-way valve, to protect the rescuer during CPR, and a separate connector for the resuscitation device. If the universal masks included in the EMK provide a means of administering CPR and also may be used with the self-inflating manual resuscitation device, then they are considered to be acceptable under both mask requirements. Therefore, a total of only three masks would be required.

9. What does "approved" EMK and "approved" AED mean?

Approved EMK means that the FAA Principal Operations Inspector assigned to the holder of an operating certificate exercises approval for the Administrator, as appropriate, of equipment to be carried aboard a certificate holder's aircraft.

Approved AED means that it is legally marketed in the United States in accordance with FDA requirements. AEDs used on airplanes must be approved by the FDA for medical use and must conform to FDA standards.

10. How can an air carrier comply with part 121, appendix A, at all times after an EMK and/or an AED is used during flight?

The regulation specifies "at least one" EMK and "at least one" AED as the minimum required on every flight for full compliance with part 121, appendix A. In the event that certain contents of an EMK are used during a flight, an inventory of the remaining contents and restocking of the contents would be needed to ensure that the minimum content requirements are met prior to any subsequent flight. For the sake of convenience, and to avoid delays, an airline may decide to overstock certain EMK items (in particular protective gloves and CPR masks), carry two EMKs, or establish a procedure for effecting one-for-one replacements as necessary.

An air carrier may elect to carry redundant equipment to ensure that after use of equipment in flight, the minimum required equipment is still on board for dispatch. In such circumstances flight attendants need to be aware of any inoperative AEDs or incomplete EMKs in the cabin in order to avoid the possibility that during an inflight medical emergency someone tries to use an inoperative AED or searches for a missing item in an incomplete EMK. In order to make flight attendants aware of inoperative equipment, an air carrier may consider the following effective practices:

- Labeling inoperative AEDs with a statement such as "Inoperative – Do Not Use"
- Labeling incomplete EMKs with a statement such as "Incomplete – Missing Contents"
- Implementing a procedure (briefing) that ensures all flight attendants are aware of incomplete EMKs or inoperative AEDs in the aircraft cabin

But, as previously noted in paragraph 5, if the air carrier elects to have only one AED and one EMK on board, if that AED is inoperative or that EMK is incomplete, the aircraft may not be dispatched.

The FAA also acknowledges that there may be circumstances that would warrant a flight attendant needing only protective gloves, a CPR mask, or both from the EMK. Accessing an

EMK for the purpose of retrieving one or both of these items could be problematic. Therefore, the FAA recommends that air carriers carry a few pairs of extra protective gloves and an extra CPR mask outside of the EMK.

The issue of AED replacement will not be as critical as EMK replacement unless, for example, an air carrier allows an AED to be taken off their aircraft for continued assistance of a passenger during emergency ground transport. Individual airlines should develop a protocol for AED use, post-resuscitation guidelines, and any AED serviceability needs**.** At a minimum, before any subsequent flights, the AED must be "operative" and there must be at least one set of unused pads with the AED. AEDs usually are packaged with a spare battery and a spare set of pads. Air carriers may want to carry extra AED pads.

11. Who is allowed to use the equipment?

Flight attendants should grant access to the equipment only to trained crewmembers or to other persons qualified and trained in the use of emergency medical equipment. The decision to allow passengers to assist another passenger and have access to medical equipment is up to the air carrier and its agents. The FAA does not attempt to define the various medical specialties under part 121 because it limits access to the extent that the only person available to assist on a flight might not be included. It would be preferable for flight attendants to check the credentials of passengers holding themselves out as medical specialists.

It is unrealistic to expect flight attendants to achieve the same level of proficiency as emergency medical personnel who perform medical procedures on a routine basis. Flight attendants should not be expected to administer medications or to start IVs. If a critical in-flight medical event occurs and a passenger medical specialist is not available, it is recommended that the sick passenger be made as comfortable as possible and the pilot in command should determine whether to attempt safe diversion of the aircraft.

As stated in the rule, the decision to offer treatment or take other action (including safe diversion of the aircraft) is discretionary with the air carrier and its agents. The FAA does not require any actions by the air carrier and its agents and/or other passengers other than having certain emergency medical equipment on board the aircraft.

12. What does "readily accessible" mean under § 121.803?

In § 121.803, the FAA uses the term "readily accessible" in the same way as the longstanding terminology used for all emergency equipment under § 121.309 (b)(2). "Readily accessible" means, as it always has, that air carriers should place equipment where crewmembers can access the equipment quickly. "Readily accessible" is not intended to mean that the emergency medical equipment should be located where it might be subject to unauthorized access.

13. Where should we store this equipment?

Because of the various configurations of aircraft, the FAA does not set one standard for storing the equipment. Airlines typically put the equipment in a locked compartment in an overhead bin, in a locked compartment attached to the bulkhead behind the last row of seats or in first class, or in an unlocked pouch attached to a bulkhead behind the last row of seats. All of these methods are acceptable. To avoid unnecessary distraction on the flight deck, and to ensure flight deck integrity, do not store AEDs in flight deck compartments.

14. How must we inspect the equipment?

You must regularly inspect emergency medical equipment in accordance with inspection periods established in your operations specifications and maintain it according to manufacturers' specification. You should follow the manufacturer's recommended procedures regarding an AED self-check.

Flight attendants perform a routine preflight inspection of all emergency medical equipment in accordance with their air carrier's procedure to assure that it is on board the aircraft, secured, and ready if needed for use. Since EMKs are sealed, it's difficult to do a comprehensive visual inspection to ascertain that no EMK items are missing or unusable; therefore, it is critical to assure EMK integrity prior to the preflight inspection stage. Any discrepancies must be resolved in accordance with your air carrier's procedures.

15. Most self-inflating manual resuscitation devices (AMBU bags) found in an EMK are accompanied by tubing that can be connected to an outlet on a portable oxygen bottle located in the aircraft cabin. This allows additional pure oxygen to mix with the ambient air in the AMBU bag and raises the level of oxygen provided during a medical event where the AMBU bag is used for respiratory support. Is this practice permissible?

Yes. Current regulations do not prohibit the connection or disconnection of oxygen masks and/or tubing that is provided with the AMBU bag in the EMK to an outlet on the regulator of an air carrier's portable oxygen bottle during a medical event that occurs in flight.

16. How often should we replace the EMK items?

The medications that must be carried in all EMKs have an expiration date of approximately 1 year: atropine, bronchodilator inhaler, dextrose, epinephrine, saline solution, and lidocaine; aspirin, non-narcotic analgesic, antihistamine, and nitroglycerine tablets. If temperature extremes occur on the aircraft at any time or if the medications have surpassed their expiration date then you should replace them. The FAA has not found expiration of medications to be problematic for air carriers under the existing requirement to carry injectable antihistamine, dextrose, epinephrine, and nitroglycerin tablets. Therefore, the FAA does not anticipate that replacing medications would become problematic by requiring additional medications of similar shelf-life. The best practice, under normal circumstances, is to replace all of the medications annually.

17. What does "damaging temperatures" mean under part 121, appendix A?

"Damaging temperatures" means temperature extremes which could alter the effectiveness of the emergency medical equipment.

Current manufacturers' specifications indicate that medications required for the EMK stored at controlled room temperature should remain stable within a temperature range of 59 to 86 degrees Fahrenheit (15 to 30 degrees Celsius). Medications carried in emergency medical vehicles, such as ambulances, reportedly remain stable within an even wider temperature range. The EMK and the aircraft cabin provide some protection from potentially harmful external temperatures. The aircraft cabin environment does not appear to negatively affect the required medications as long as they are replaced before their expiration date.

If an aircraft has been exposed to extremes of hot or cold temperatures, the medications in a liquid form (injectable) should be inspected before use. If they are yellow or cloudy, then they may have lost their effectiveness and should not be used. In general, once injectable medications are frozen they should not be used, and high, prolonged heat will degrade the efficacy of most medications.

In addition, the AED, batteries, and defibrillator pads usually have a recommended temperature range for storage and operation. These temperature ranges vary between manufacturers, but are generally much wider than for the medications. The manufacturers' specifications should be consulted for proper handling procedures if the aircraft cabin exceeds the recommended temperatures. Prolonged exposure to temperatures outside the recommended limits may damage the batteries or may cause the pads to not adhere properly.

If an aircraft is parked or taken out of service for an extended period of time in a location where it may be exposed to temperature extremes, then the emergency medical equipment should be taken off the aircraft and protected.

18. Since some air carriers carry EMKs that may contain controlled substances, how can they be transported legally? Is transporting these substances compatible with Drug Enforcement Administration (DEA) regulations?

Although the FAA does not require any controlled substances for the EMK, some air carriers may purchase commercial EMKs that are prepackaged with a controlled substance(s) (for example, diazepam). Such EMKs cannot be purchased (or carried) unless a current DEA Registration Certificate is on file with the EMK distributor. If a controlled substance is compromised (e.g., lost, stolen, or missing) the air carrier must report it to the DEA.

19. Does the FAA regulate safety standards for AEDs?

No. The FDA is responsible for regulating safety standards for the manufacture and use of AEDs. The FAA is responsible for regulating the safety of the power sources used in AEDs when carried on board a passenger-carrying aircraft. You should direct any questions about

AEDs directly to the manufacturer and/or to the FDA Center for Devices and Radiological Health. AED manufacturers may have resources available to provide the FDA-required oversight.

For safety purposes, the FAA asks that certificate holders comply with the guidance in applicable Flight Standards Information Bulletins for Airworthiness, such as FSAW 98-05, Medical Portable Electronic Devices (PED). Certificate holders must also comply with the requirements of applicable FAA Technical Standard Orders (TSO) such as TSO-C142, Lithium Batteries. The devices should be maintained in accordance with manufacturers' specifications and should be inspected in accordance with schedules developed under operations specifications. Currently, AEDs are powered by primary (not rechargeable) lithium batteries. Safety of these batteries is stressed because extremely energetic materials are used in lithium cells and they are not intrinsically safe. Safety concerns include the possibility of fire, explosion, and the venting of toxic or flammable gases.

20. What are acceptable power sources for AEDs?

The FAA requires the power source (e.g., batteries) used to power AEDs to comply with all requirements in applicable advisory material such as Advisory Circular 91.21-1A Use of Portable Electronic Devices Aboard Aircraft (http://www.airweb.faa.gov/Regulatory_and_Guidance_Library/rgAdvisoryCircular.nsf/MainFrame?OpenFrameSet)), and in applicable TSOs, such as TSO-C142, Lithium Batteries (http://avinfo.faa.gov/tso/tsocur/current.htm).

On March 24, 2005, the FAA amended the regulations for emergency medical equipment to allow approved power sources that do not have TSO markings to be used in AEDs carried onboard aircraft (http://dmses.dot.gov/docimages/p80/322276.pdf). AED power sources manufactured before July 30, 2004, and not TSO marked, may continue to be used until their expiration date, provided that the power source manufacturer has requested and received from the FAA a finding of TSO equivalency for its product.

Specifically, part 121, Appendix A, was amended to allow the use of AED power sources that were manufactured before July 30, 2004, and do not have the TSO marking required, provided that the manufacturer of the power source has received a finding of equivalency from the appropriate Aircraft Certification Office (ACO). A manufacturer can seek this determination by contacting the ACO that issued the TSO approval of its AED power source.

21. Is labeling an AED with the statement "approved for use on aircraft" appropriate?

No. Arbitrary use of the statement "approved for use on aircraft" is not appropriate. It could lead to a safety problem because toxic gas venting precautions are required before placing AEDs containing lithium sulfur dioxide batteries in an airplane cabin. The battery manufacturer must supply a note with the batteries that addresses installation procedures and limitations. Marking requirements for lithium batteries are defined in part 21, specifically § 21.607(d).

22. What prompted requirements for emergency medical equipment?

The Aviation Medical Assistance Act (the Act) of 1998 [Pub. L. 105-170, 49 U.S.C. 44701] directed the FAA to determine whether current minimum requirements for air carrier emergency medical equipment and air carrier crewmember emergency medical training should be modified. As directed in the Act, the FAA conducted a year-long data collection on death or near-death in-flight medical events. It revealed 188 total events resulting in 108 deaths (119 of these 188 total incidents were cardiac-related resulting in 64 deaths). For cardiac-related events on the aircraft, an AED was reported as "not available" for 40 events. An AED was available and used to deliver at least one shock in 17 separate events. From these events, four passengers were reported as having survived. Subsequent to the data collection, further investigation revealed that more passengers, and a flight crewmember, had also survived after having been shocked with an AED. Based on these events, it was determined that part 121 should be amended to require emergency medical enhancements, such as performance-based training for flight attendants on the use of AEDs and CPR, enhanced EMKs, and AEDs.

ORIGINAL SIGNED BY
CHESTER D. DALBEY (for)

James J. Ballough
Director, Flight Standards Service

Advisory Circular

Subject: EMERGENCY MEDICAL EQUIPMENT TRAINING

Date: 1/12/06

Initiated by: AFS-220
AAM-210

AC No: 121-34B

1. What is the purpose of this advisory circular (AC)?

This AC provides guidance regarding crewmember training programs (flight attendant training programs in particular) that incorporate Automated External Defibrillators (AED) and enhanced Emergency Medical Kits (EMK). The FAA expects and anticipates some variation among the training programs air carriers establish for crewmember emergency medical training. (Also see AC 121-33B, Emergency Medical Equipment.)

2. Does this AC supersede any existing ACs?

This AC supersedes AC 121-34A, Emergency Medical Equipment Training, dated May 9, 2003. It also relates to existing AC 120-44A, Air Carrier First Aid Programs (http://www.faa.gov/avr/afs/cabinsafety/acidx.cfm), which is also a good reference source.

3. What FAA regulations does this AC cover?

Title 14 of the Code of Federal Regulations (14 CFR) part 121, subpart X; part 121, appendix A. (http://www.gpoaccess.gov/ecfr).

4. Who should read this AC?

FAA aviation safety inspectors (cabin safety and operations), part 121 air carrier certificate holders, directors of operations, directors of safety, crewmembers, AED manufacturers and suppliers, EMK suppliers, as well as people involved in the development of air carrier procedures and training programs. This AC may also be valuable to people associated with operations under 14 CFR part 125, part 135, and subpart K of part 91 (fractional ownership programs).

5. What emergency medical equipment training must the certificate holder provide to all crewmembers?

All crewmembers must receive initial and recurrent training on the following:

- Emergency medical event procedures, including coordination among crewmembers.
- Location, function, and intended operation of emergency medical equipment.
- Recognizing EMK content. (This instruction for flight attendants would also need to include the requirement to coordinate with the Captain regarding what items might need to be replaced at the end of a flight if an EMK is used during a flight. All crewmembers must understand that EMKs and AEDs are “no-go” items and must be carried as indicated on the Minimum Equipment List.

6. What training must the certificate holder provide only to flight attendants?

In addition to the initial and recurrent training described in paragraph 5, flight attendants must receive the following:

- Initial instruction, to include performance drills, in the proper use of AEDs.
- Initial instruction, to include performance drills, in Cardiopulmonary Resuscitation (CPR).
- Recurrent training, to include performance drills, in the proper use of AEDs and in CPR at least once every 24 months.

7. Does the FAA require a standard curriculum?

No. The FAA does not require a standard curriculum or standard testing. Instruction should conform to national programs such as those offered by the American Heart Association or the American Red Cross. (For information about these national programs, contact the local chapters of these organizations.) The intent of the rule is to allow air carriers to incorporate training on these specific subjects into the context of their approved training programs. There is no requirement for separate curricula or separate knowledge tests.

8. Does the FAA require specified hours of instruction?

No. The FAA does not require a minimum number of program hours for emergency medical equipment and procedures training contained in crewmember emergency training or flight attendant recurrent training. Although times may vary between programs, the American Heart Association curriculum combining Basic Life Support (BLS) and AED training requires approximately 3½ to 4 hours as does subsequent recurrent training. BLS training may be conducted separately from the AED instruction or in a combined session. (It should be noted that BLS instruction does not necessarily need to lead to official BLS certification.)

Many air carriers conduct performance drills in CPR and proper use of AEDs during recurrent training once every 12 months, which is desirable. (Some air carriers may also conduct performance drills in BLS once every year.) Because the FAA does not want to deviate from existing practice by establishing a separate training schedule for "hands-on" performance drills for recurrent training for flight attendants, the performance drills in CPR and proper use of AEDs are required for flight attendants once every 24 months.

9. What issues should we address in an emergency medical training program?

- A segment on personal procedures protecting against blood-borne pathogens is recommended. (This guidance is elaborated in AC 120-44A.)
- The need for CPR and an AED whenever the passenger is breathless, pulseless, and unconscious.
- The difference between a heart attack (myocardial infarction or MI) and cardiac arrest (ventricular fibrillation) and similar events (e.g., stroke).
- An introduction to the concept of the "Chain of Survival" (Access to Care, Early CPR, Defibrillation, Advanced Cardiac Care).
- The importance of practical CPR skills as a necessary part of care.
- Information regarding medications in the EMK (as discussed under paragraphs 6 and 7 of AC 121-33B) and what qualified health care professionals might use them for.
- Passenger-specific issues (e.g., when to discontinue resuscitative measures; ground transport issues; do-not-resuscitate orders and living wills; post-incident analysis and discussion).
- Protocols for responding to passengers when no onboard voluntary, professional medical assistance is available.
- The ability to contact and coordinate with ground-based medical care providers, if available.
- That no oxygen (including portable oxygen bottles, portable oxygen concentrators, compressed oxygen cylinders and aircraft oxygen systems) should be used within 10 feet of an AED at the moment the AED is being used to deliver a shock to a person.

10. What venue is most appropriate for conducting instruction?

Simulated AED practice scenarios should, to the greatest extent possible, take place in the cabin environment. This venue is most appropriate for drilling problems that may be encountered when flight attendants assist stricken passengers within the confines of an aircraft cabin.

11. Who should provide the instruction?

Training instructors who are certified in BLS instruction. If you need to find a certified BLS instructor, contact the local chapter of the American Heart Association or American Red Cross.

12. How many participants should be in a given session?

During the portion of training where there is a "hands-on" application of practical skills, we recommend no more than 15 students per instructor.

13. Is physician oversight necessary?

While close supervision by a physician is not necessary, it is advisable to have a physician oversee the training program to maintain minimum quality standards. In many cases, this physician may be the airline medical director; however, it may vary with different circumstances.

14. Who is covered under "Good Samaritan" protection?

The Aviation Medical Assistance Act of 1998 covers liability to the extent defined as follows (quoted verbatim from the Act):

"**(a) Liability of Air Carriers.** An air carrier shall not be liable for damages in any action brought in a Federal or State court arising out of the performance of the air carrier in obtaining or attempting to obtain the assistance of a passenger in an in-flight medical emergency, or out of the acts or omissions of the passenger rendering the assistance, if the passenger is not an employee or agent of the carrier and the carrier in good faith believes that the passenger is a medically qualified individual.

"**(b) Liability of Individuals.** An individual shall not be liable for damages in any action brought in a Federal or State court arising out of the acts or omissions of the individual in providing or attempting to provide assistance in the case of an in-flight medical emergency unless the individual, while rendering such assistance, is guilty of gross negligence or willful misconduct."

Air carriers should address their employees concerning the company policy on the provision of medical assistance to passengers. While an employee who chooses to provide assistance may be protected under Federal law from claims from passengers, the company may or may not have a policy of providing legal protection. Employees also should understand that they may be subject to disciplinary action if found in violation of company policy. There is no obligation under Federal law to provide medical assistance to passengers. The FAA does not have the authority to require employees to provide assistance or to defend employees sued for acts or omissions in the performance of duties.

15. What is the FAA's position regarding the air carrier and its agents choosing to offer medical assistance to passengers during critical phases of flight (such as during landing)? (For example, § 121.391 requires flight attendants to be located as near as practicable to required floor level exits during takeoff and landing.)

The goal of all FAA regulations is to maintain a safe flying environment for all passengers and crew. Emergency situations could occur in flight that may affect the ability of the crewmembers or the passengers to comply with FAA regulations, such as those that require them to be secured in a specific location. An example of such a situation is a flight attendant deciding to administer CPR to a passenger during landing. Air carriers should develop procedures regarding such situations and incorporate them into its crewmember's manuals and training programs.

Procedures should address the airline's policy toward the following: expected crewmember performance; efficient communication and coordination among crewmembers; passenger briefing procedures (if needed); protocols for requesting assistance from medically qualified passengers (if needed); even distribution of flight attendants throughout the cabin; and, in the case of one flight attendant on board, procedures to ensure that the safest cabin environment possible is maintained.

16. What prompted requirements for emergency medical enhancements?

The Aviation Medical Assistance Act (the Act) of 1998 [Pub. L. 105-170, 49 U.S.C. 44701] directed the FAA to determine whether current minimum requirements for air carrier emergency medical equipment and air carrier crewmember emergency medical training should be modified. As directed in the Act, the FAA conducted a year-long data collection on death or near-death in-flight medical events. It revealed 188 total events resulting in 108 deaths (119 of these 188 total incidents were cardiac-related resulting in 64 deaths). For cardiac-related events on the aircraft, an AED was reported as "not available" for 40 events. An AED was available and used to deliver at least one shock in 17 separate events. From these events, four passengers were reported as having survived. Subsequent to the data collection, further investigation revealed that more passengers, and a flight crewmember, had also survived after having been shocked with an AED. Based on these events, it was determined that part 121 should be amended to require emergency medical enhancements, such as performance based training for flight attendants on the use of AEDs and CPR, enhanced EMKs, and AEDs.

ORGINAL SIGNED BY
CHESTER D. DALBEY (for)

James J. Ballough
Director, Flight Standards Service

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

September 2, 2022

Olare Nelson
U.S. Office of Special Counsel
1730 M Street, Suite 300
Washington, DC 20036-4505
onelson@osc.gov

OSC Matters: DI-18-5205 and DI-19-0778
TSA Supplemental Information Provided in Response to OSC Request

1. **The allegations OSC referred were based on a substantial likelihood of gross mismanagement, and a substantial and specific danger to public health and safety. However, the agency's report only explicitly addressed the allegations in the referral as a possible violation of a law, rule, or regulation. We ask that the agency's report, at minimum, state whether it substantiates the original allegations referred.**

TSA's report explicitly speaks to the five required factors in 5 U.S.C. §1213(d). While the report addresses the statutorily required factors, the evidence does not demonstrate gross management or a substantial and specific danger to public health and safety for either disclosure. As stated in TSA's June 15, 2020 response, "The investigation revealed that TSA did not engage in a failure to protect flight crews and the public or a failure to prevent significant security breaches. Rather, TSA has addressed and continues to address each of these issues."

2. **<u>Weaponized Opioids</u>**
   a. **The report and supplemental report mention that Security Vulnerability Management Process evaluation(s) have been completed to assess the risk of fentanyl being released in the civil aviation sector. The report appears to distinguish between the Security Vulnerability Management Process evaluation, which has been done, and an Enterprise Risk Management (ERM) evaluation, which has not been done, although the report touts the agency's ability to do an ERM. *(See Supp. Report p. 3, para. 2).***

To clarify, Enterprise Risk Management (ERM) is a comprehensive approach to risk management that engages organizational systems and processes together to improve the quality of decision making for managing risks that may hinder an organization's ability to achieve its objectives. ERM provides a framework to address TSA's full spectrum of risks in the most effective manner. The Executive Risk Steering Committee (ERSC) is the governing body within the ERM framework that retains overarching responsibility for defining strategy and managing risk at an enterprise level. Thus, an "ERM evaluation" means that the potential risk has been reviewed by the ERSC.

The Security Vulnerability Management Process (SVMP) is one component of the ERM framework. Vulnerabilities assessed by the SVMP may be briefed to the ERSC.

In the summary of the report of investigation for this case, which the Agency provided in its initial response, the Agency stated that the action "taken or planned as a result of the investigation" is that it would submit the report of investigation into the SVMP, in the TSA Enterprise Performance and Risk office, for evaluation and consideration of the risk of fentanyl being released in the civil aviation sector. TSA submitted the report as indicated. It was evaluated by the SVMP on February 19, 2020 and it was briefed through the ERSC on February 19, 2020.

i. **Please detail the differences between these evaluations, including the pros and cons of each, and explain why the agency has not chosen to conduct an ERM (which the report suggests is a more thorough and formal evaluation).**

As stated above, the risk of fentanyl/opioids has been evaluated through the ERM framework because it was reviewed by the ERSC.

TSA established an Enterprise Risk Management (ERM) program to provide a comprehensive, structured, and consistent approach to risk management to improve the quality of decision making for managing risks. ERM provides TSA with a means to align strategy, resources, and technology for the purpose of addressing and managing uncertainties in executing our counterterrorism mission. The ERM is a discipline, focused on integrating organizational risks into an enterprise-wide, strategically-aligned portfolio view.

The SVMP is one piece of the ERM. The SVMP utilizes a framework to manage security risks and vulnerabilities. The SVMP process is focused on operational vulnerabilities, which can be identified by any Program Office. The ERSC, a key component of ERM, is composed of the Chief Risk Officer and Assistant Administrators and oversees the development and implementation of processes used to identify, analyze, prioritize, and address risks across TSA. One of their responsibilities is to conduct continuous monitoring and reporting of risk across the Agency, including reviewing the SVMP tracker report on a quarterly basis.

ii. **Further, we are requesting sufficient information about these evaluations so that we can appropriately assess the reasonableness of the agency's actions. *(See Report p. 7, para. 2)***

Please see attached ERM Manuals, dated February 2019, and the previous version dated March 2016. The ERM Manual was updated in 2019 to reflect changes in organizational structure, a new TSA strategy under Administrator Pekoske, an updated maturity model, and to incorporate OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, released July 15, 2016. Please also see attached TSA SVMP Charter dated September 6, 2019 and TSA Management Directive 4101, *Enterprise Risk Management.*

b. **The report also mentions that it has not evaluated the risk of a fentanyl/opioid attack on board an aircraft but that it has processes in place to do so if the need arises.**

   i. **What are those processes? What type of "need" would trigger those processes?**

TSA has evaluated this risk. The risk of a fentanyl/opioid attack on board an aircraft was evaluated by the SVMP and briefed through the ERSC on February 19, 2020.

In addition to the ERSC briefing and the SVMP evaluation, TSA's Intelligence and Analysis (I&A) reported that I&A had researched the threat of opioids, and the analysts found nothing to support the idea that terrorists have considered or are considering either opioids or foods trucks as a method of attack. See attached memo dated May 7, 2019.

ii. **Is the agency relying only on the 2017 TSA Intelligence and Analysis? Given the age of the report and the speed with which risks can evolve, is the agency relying on any other information or reports? Alternatively, in the intervening years, has the agency evaluated the risk? If so, what were the results and what actions were taken as a result? (See Report p. 7, para 2).**

As stated in the above answer, TSA evaluated the risk after 2017, in both 2019 and 2020.

c. The supplemental report notes that it does three types of testing and indicates that these forms of testing can detect miniscule amounts of opioid powders. *(See Supp. Report p. 2 final para).* Yet, the supplemental report seems to indicate that extra testing may only be performed on quantities of powder greater than 12 oz./350 ml.

i. Does the normal screening sufficiently detect smaller quantities of opioids such that "extra" screening is not warranted? If yes, how so?

TSA's screening procedures are focused on security and are designed to detect potential threats to aviation and passengers. Accordingly, TSA security officers do not search for illegal drugs. Regardless of the amount, if a Transportation Security Officer (TSO) finds a powder that could be fentanyl, a fentanyl analogue, or anything otherwise suspicious during screening, he or she does not open the container or conduct additional screening of the powder. The TSO is to refer the matter to a supervisor, who will notify a law enforcement officer.

To protect TSOs from potential exposure during the screening process, TSA approved equipping TSOs with thicker 5 mil nitrile gloves on June 13, 2017. TSA also issued National Shift Briefs on June 3, 2017, February 24, 2018, July 11, 2018, October 31, 2018, and November 2, 2018, which provided information regarding Fentanyl.

Extra screening of powders during the screening process may occur when quantities of powder exceed 12oz. To test powder, only a miniscule amount of the powder is required as the sample. For Explosive Trace Detection (ETD) equipment, the amount needed for a test is a fingerprint; the amount is not visible to the Human Eye. For colorimetric testing, a few visible grains are needed on the swab. The swab is "sticky" so it will pick up and hold onto the grains. Regardless of quantity, if a TSO believes there may be a powder during screening that could be fentanyl, the TSO will refer the matter to a supervisor, who will notify a law enforcement officer.

Thus, TSA has procedures in place to prevent fentanyl/opioids from entering an aircraft. However, if fentanyl/opioids were to enter the aircraft, the risk of them being used to overtake an airplane is low for several reasons. First, TSA's Intelligence and Analysis (I&A) reported on May 7, 2019 that I&A had researched the threat of opioids in, and the analysts found nothing to support the idea that terrorists have considered or are considering opioids as a method of attack.

Second, the ability of a passenger to release fentanyl into the cockpit is extremely limited due to the measures in place to protect the cockpit against intrusion. The Federal Aviation Administration has issued standards for the strengthening of cockpit doors to protect cockpits from forcible intrusion and small-arms fire or fragmentation devices, such as grenades. See 14 CFR part 25.795.

A FAA-issued rule requires a means for flight crews to visually monitor the door area outside the flight deck and that flight attendants have a means to discreetly notify the flight crew of suspicious activity or security breaches in the cabin. See 72 CFR part 45629; 14 CFR part 121. Further, in 2015 the FAA issued Advisory Circular No. 120-110, *Aircraft Secondary Barriers and Alternate Flight Deck Security Procedures,* providing guidance on three acceptable methods of secondary flight deck security: installation of physical secondary barriers, use of improvised non-installed secondary barriers, and human secondary barriers. These protocols provide protective, anti-intrusion benefits to the cockpit. All aircraft carriers are in compliance with the Advisory Circular by utilizing one of the three methods of flight deck security.

Third, even in the extremely unlikely case that a passenger could get fentanyl into the cockpit, and appropriately aim the powder to hit the pilot, throwing fentanyl at the pilot would not likely incapacitate them. Experts from the American College of Medical Toxicology agree that fentanyl is "not absorbed well enough through the skin to cause sickness from incidental contact." They noted, even an "extreme example illustrates that even a high dose of fentanyl prepared for transdermal administration cannot rapidly deliver a high dose." *See* https://www.acmt.net/cgi/page.cgi/_zine.html/Press_Releases/ACMT_Position_Statement_on_Fentanyl_Exposure. In other words, if a pilot has some on their skin, he or she can brush it off, and it will not pass through the skin quickly enough to cause intoxication.

Lastly, as stated in the report previously provided to OSC, former Department of Defense Research Chemist, Dr. Christina Baxter, and Don Ostrowski of Federal Resources, indicted that if the fentanyl was released near passengers, the passenger closest to the release may be affected, however, the ventilation system on most aircrafts include filters that would collect the fentanyl particulates, reducing the possibility of recirculation, and would not affect the rest of the aircraft. If this were to occur, it is recommended that the flight crew is supplied air as soon as possible.

ii. **Has the agency conducted testing to determine its success rate in detecting small quantities of opioids? If so, what is the agency's success rate in detecting such miniscule amounts using its current methods? If not, please explain.**

TSA's screening procedures are focused on security and are designed to detect potential threats to aviation and passengers. Accordingly, TSA security officers do not search for illegal drugs.

3. **Religious Food Trucks**
   a. **The report mentions that TSA is positioned to formally assess the efficacy of the airport catering security protocols, but that it has chosen not to do so despite its admission that insider threats are the biggest vulnerability. *(See Report p. 10).***
      i. **Please explain why TSA has chosen not to conduct such an assessment.**

To clarify, the report indicates that there is an insider threat risk throughout the transportation sector. The report also indicates that due to the insider risk regarding catering, TSA has a layered approach to secure catering trucks. It is worth noting that Mr. MacLean's unauthorized attempt to break the seal of the catering cart was unsuccessful due to TSA's security measures.

There are multiple processes in place to mitigate the risk. First, the regulations and policies that outline how aircraft operators must secure the catering for their flights are as follows:

- Code of Federal Regulations (CFR) 49 CFR §1540, §1544 and §1546;

- Aircraft Operator Standard Security Program (AOSSP) Chapter 10 for domestic air carriers; and
- Emergency Amendment (EA) 1546-12-07L for foreign air carriers.

These regulations and policies include requirements for securing catering carts when they are being "made up" at the catering facility and when the catering carts are being transported to the aircraft. All catering carts and catering supplies are visually inspected by the aircraft operator (or authorized representative) to look for items that do not belong. The visual inspection is limited by local laws and hygiene standards. After the visual inspection, the air carrier must randomly pull food trays to look for signs of tampering.

Additionally, catering trucks are subject to a robust security and screening program that includes rules regarding sealing, monitoring, inspecting and testing.

Regarding the catering security personnel, the domestic air carrier security program (AOSSP Chapter 10) requires that individuals performing the catering security functions required by the program have an airport-issued or approved identification media, which requires fingerprint-based criminal history records check (CHRC) and a security threat assessment (STA).For foreign air carriers, TSA requires the catering security personnel either have an airport-issued identification (and the required CHRC and STA) or they must have the employee provide 10 years of employment history and the foreign air carrier must verify the most recent 5 years of employment. There is no TSA requirement for the catering personnel to have a background check.

TSA's Security Operations Compliance Division is responsible for ensuring regulated entities are complying with Federal regulations and agency policies. Compliance has conducted over 4,000 catering inspections since the beginning of FY2020, with an extremely high compliance rate for catering.

b. Please provide us with a copy of the report regarding the 2018 Aviation Security Advisory Committee (ASAC) insider threat review that was conducted. We would like to understand the areas evaluated in that review that are relevant to the allegations in the referral.

TSA is unable to provide this report without including Sensitive Security Information (SSI).

c. The agency report states that as of February 2020, TSA was considering implementing some of ASAC's recommendations.

i. What were those recommendations? Were they ultimately implemented? If not, please explain. ***(See Report p. 10, 2nd to last para.)***

TSA is unable to provide the recommendations without including SSI. The ASAC report included five recommendations regarding insider threats of aviation workers, which, depending on the recommendation and the circumstances, may apply to catering companies. For example, the applicability may depend on whether the catering company is located on airport property. Two of the recommendations were completed, and three are still open and have not been completed yet.

Transportation Security Administration

Enterprise Risk Management (ERM)

Policy Manual

February 2019

Transportation
Security
Administration

Contents

DOCUMENT CONTROL INFORMATION

Document name	TSA Enterprise Risk Management (ERM) Policy Manual
Document author	TSA Chief Risk Officer
Document version	Version 3
Document status	Draft
Date released	

Document edit history

Version	Date	Additions/modifications	Prepared/revised by
1.0	August 2014	Initial Release	OCRO
2.0	January 2016	Update	OCRO
3.0	February 2019	Update	SP&I

Document review/approval history

ABBREVIATIONS

The following abbreviations are used throughout the document for conciseness:

AA	Assistant Administrator
CMM	Capability Maturity Model
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CRO	Chief Risk Officer
DHS	Department of Homeland Security
ERM	Enterprise Risk Management
EAA	Executive Assistant Administrator
ERSC	Executive Risk Steering Committee
GAO	U.S. Government Accountability Office
GPRA	Government Performance and Results Modernization Act
HSE	Health, Safety, and Environment
ISO	International Standards Organization
IPT	Integrated Project Team
KPI	Key Performance Indicators
KRI	Key Risk Indicators
PAR	DHS Performance Accountability Report
PII	Personally Identifiable Information
RM	Risk Management
RBS	Risk Based Security
SLT	Senior Leadership Team
SME	Subject Matter Expert
SP&I	Strategy, Policy Coordination, and Innovation
SSI	Sensitive Security Information
TSA	Transportation Security Administration
MRKC	Mission Risk Knowledge Center

INTRODUCTION

TSA established an Enterprise Risk Management (ERM) program to provide a structured, disciplined, and consistent approach to risk management that facilitates risk-informed decision making throughout the organization. ERM provides TSA with a means to align budget, strategy, processes, people, and technology for the purpose of evaluating and managing uncertainties in executing our counterterrorism mission. A consistent approach to risk management across the organization is essential for TSA leaders to identify and prioritize strategic risks amidst a tight budget environment. ERM enables TSA to more effectively manage enterprise level risks, and it enables agency leaders to consider the trade-offs between risks, associated costs, and value creation across the organization.

This manual explains TSA's foundational elements of its ERM program and ERM roles and responsibilities of entities at TSA in implementing ERM. As TSA's Executive Director for Strategy, Policy Coordination and Innovation, I have approved this approach to implementing ERM as the path to achieve mature and sustainable ERM activities and processes. By consistent use of ERM across the organization, TSA will be positioned to identify and assess risks within the current environment through a systematic process which evaluates the impact of risk on TSA's ability to achieve our mission and objectives in support of U.S. Department of Homeland Security (DHS) strategic objectives.

[redacted]
Executive Director,
Strategy, Policy Coordination and Innovation (SP&I)

PURPOSE OF THIS DOCUMENT

TSA's Enterprise Risk Management Policy Manual (ERM) Policy Manual has two core purposes. First, the ERM Policy Manual defines the foundational elements of TSA's ERM program: TSA's ERM Policy Statement, Risk Appetite Statement, Risk Taxonomy, ERM Framework, and risk management governance structure.

Second, the ERM Policy Manual details the specific roles and responsibilities of TSA leadership, Executive Assistant Administrators, TSA offices, risk management staff, and all TSA employees in implementing ERM throughout the agency. Through the Risk Appetite Statement, the ERM Policy Manual provides guidance to TSA leadership on aligning resource and policy decisions to the amount of risk TSA is willing to accept/pursue within a specific area. Specific details for each of the steps in the ERM framework, along with various risk management tools techniques, and assessment scales are provided in the accompanying ERM Practitioners Guide for use by TSA offices and risk management staff.

The contents of this document provide the evolving blueprint for TSA's ongoing ERM program. Updates to the Policy Manual will be made as the ERM program matures.

- Establish clear accountability and ownership of risk.
- Develop the capacity for continuous monitoring and reporting of risk across the Agency from the operational level to the Executive Risk Steering Committee (ERSC).
- Develop a common language and consistent approach across all TSA offices that help to establish the broad scope of risk and to organize risk management activities and reinforces TSA's risk culture.
- Ensure that risks are managed in a manner that maximizes the value TSA provides to the Nation consistent with defined risk appetite and risk tolerance levels.

TSA recognizes that many risks within the organization are interrelated and cannot be effectively and efficiently managed independently within a given TSA office. Instead, these interconnected risks facing TSA must be managed across the organization and, in many instances, in tandem between the agency and its stakeholders. This manual sets forth guidance in the form of repeatable processes and activities to identify, analyze, evaluate, and respond and effectively manage the risks to TSA's mission.

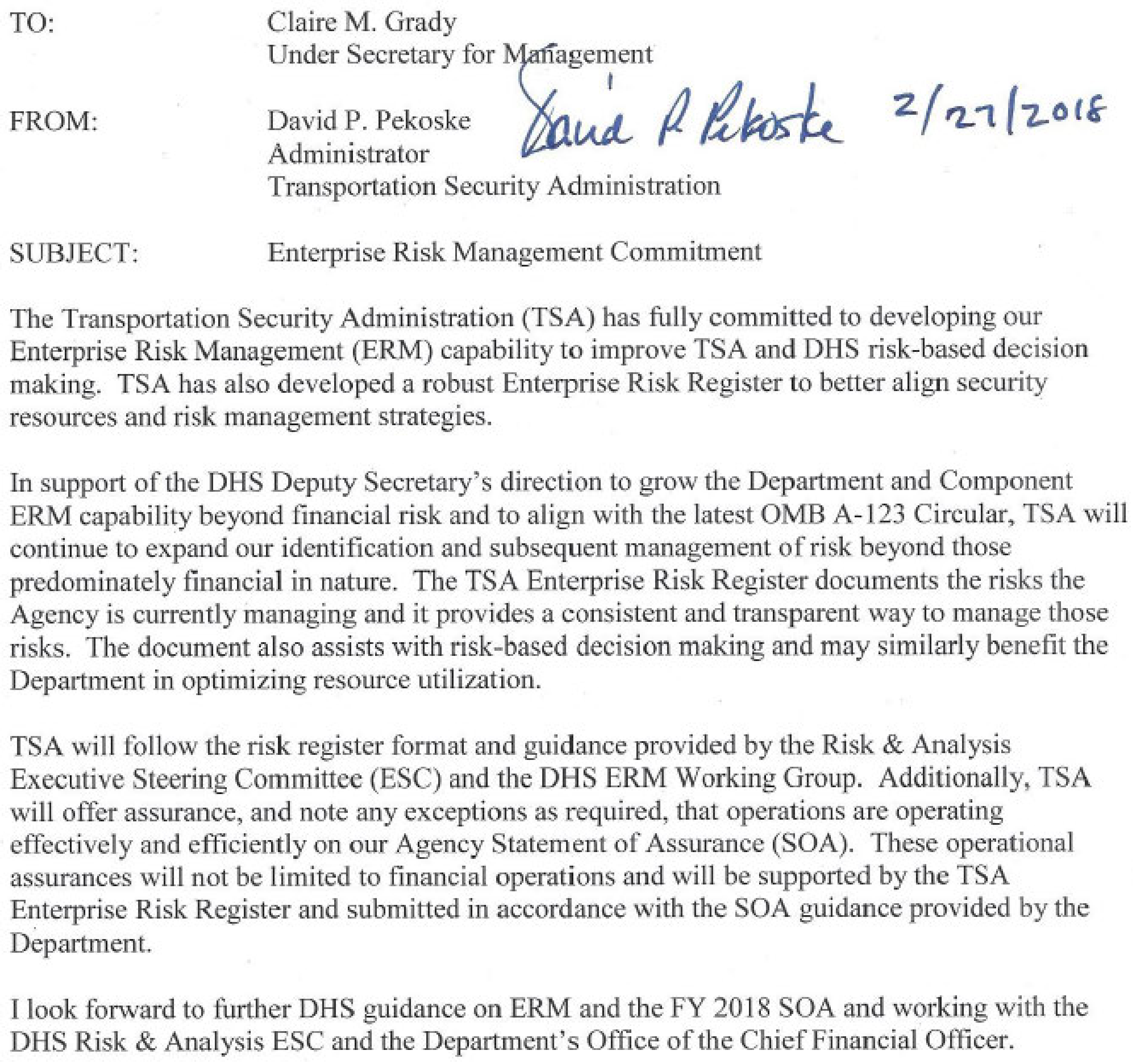
ERM OBJECTIVE

TSA's ERM framework provides the means to embed risk management as a core competency in TSA programs, enabling the agency to fully embed robust and consistent risk management practices at both the enterprise-wide level and within each TSA office in a way that facilitates risk-informed decision making at all levels.

The ERM objectives are to:

- Support TSA leadership through transparency and insight into risks that could impact the ability to execute TSA's mission through the implementation of well-defined and common risk management processes, tools, and techniques.
- Quickly identify both current and emerging risks and develop plans to respond to risks as well as to take advantage of opportunities.
- Increase the likelihood of success in achieving the objectives of TSA's mission and the DHS Strategic Plan.
- Build credibility and sustain confidence in TSA's governance and risk management by all stakeholders including industry, federal, state, and local partners, and the American people.
- Improve the understanding of interactions and relationships between risks.

ENTERPRISE RISK MANAGEMENT COMMITMENT



TO: Claire M. Grady
Under Secretary for Management

FROM: David P. Pekoske David P Pekoske 2/27/2018
Administrator
Transportation Security Administration

SUBJECT: Enterprise Risk Management Commitment

The Transportation Security Administration (TSA) has fully committed to developing our Enterprise Risk Management (ERM) capability to improve TSA and DHS risk-based decision making. TSA has also developed a robust Enterprise Risk Register to better align security resources and risk management strategies.

In support of the DHS Deputy Secretary's direction to grow the Department and Component ERM capability beyond financial risk and to align with the latest OMB A-123 Circular, TSA will continue to expand our identification and subsequent management of risk beyond those predominately financial in nature. The TSA Enterprise Risk Register documents the risks the Agency is currently managing and it provides a consistent and transparent way to manage those risks. The document also assists with risk-based decision making and may similarly benefit the Department in optimizing resource utilization.

TSA will follow the risk register format and guidance provided by the Risk & Analysis Executive Steering Committee (ESC) and the DHS ERM Working Group. Additionally, TSA will offer assurance, and note any exceptions as required, that operations are operating effectively and efficiently on our Agency Statement of Assurance (SOA). These operational assurances will not be limited to financial operations and will be supported by the TSA Enterprise Risk Register and submitted in accordance with the SOA guidance provided by the Department.

I look forward to further DHS guidance on ERM and the FY 2018 SOA and working with the DHS Risk & Analysis ESC and the Department's Office of the Chief Financial Officer.

TSA RISK APPETITE STATEMENT

The Transportation Security Administration (TSA) risk appetite statement provides broad guidance regarding the amount of risk within a specific area that TSA is willing to accept/pursue in maximizing the value TSA provides to the American people. Risk appetite is considered in different ways depending on whether the risk (uncertainty) being considered represents a dynamic threat or an opportunity. When considering dynamic threats (unwanted outcomes), risk appetite defines the level of exposure that TSA considers is tolerable. In these instances, TSA will mitigate risk through tight management controls or cautious/conservative policy decisions. Conversely, when considering opportunities (creating or enhancing value), risk appetite defines how much TSA is willing to put at risk in order to realize the desired benefits. In these situations, TSA implements control actions to prevent potential negative impacts from exceeding the level deemed allowable and to monitor if the desired outcomes are being realized. The risk appetite definitions in the following figure help describe the spectrum for the agency's various levels of risk appetite.

Risk Appetite Definitions

Risk Appetite Approach	Risk Averse	Risk Neutral	Risk Tolerant
Level Of Risk Taking Versus Reward	TSA takes a cautious approach to risk and seeks to avoid negative consequences. TSA sets tight risk tolerance limits, focuses on value preservation, and seeks to minimize risk levels to as low as reasonably practicable.	TSA takes a balanced approach between risk taking and value creation. For risks without great upside or downside potential, TSA sets moderate risk tolerance limits and seeks to avoid over-control.	TSA takes calculated risks to achieve strategic objectives and create additional value. TSA sets wider risk tolerance limits and is willing to accept greater than normal risks to achieve the benefits.
Risk Response Decision Criteria	Minimal calculated risk is accepted. Mitigation actions are taken even though the costs may be greater than the expected consequence should risk manifest. Employ tight management controls to reduce uncertainty and preserve current value, with cautious and conservative policy decisions.	TSA accepts calculated risks with risk response actions determined based on cost effectiveness, management priorities, and potential outcomes. Management controls are implemented to monitor cost effectiveness and if desired outcomes are being achieved.	Risk response actions are taken to prevent potential losses from exceeding a maximum allowable loss. Controls are implemented to monitor that desired outcomes are being realized.

TSA creates value by protecting the Nation's transportation systems while enabling the movement of legitimate travelers and goods. TSA seeks practical and cost-effective solutions to effectively reduce the most significant risks to TSA's ability to achieve its mission.

TSA has different appetites for different risk types expressed in the following statements:

- TSA is averse to security risks that could result in catastrophic consequences.
- TSA is averse to the compromise of classified information.
- TSA is averse to the compromise of Sensitive Security Information (SSI) and Personally Identifiable Information (PII).
- TSA is averse to workforce-related risks pertaining to integrity, performance, health and safety, and regulatory compliance.
- TSA is risk neutral to events that could damage its standing and reputation with the traveling public, US Congress, and other Federal, industry, and international stakeholders.
- TSA is risk neutral with regard to other mission and business operational risks.
- TSA is risk tolerant with respect to programs that enhance the movement of legitimate travelers and goods, including supporting acquisitions, technologies, policies, and operational procedures.
- TSA is risk tolerant to efforts that deny exploitation of the Nation's transportation systems for nefarious purposes.

TSA makes risk-informed decisions to achieve its mission within the parameters of its risk appetite:

- TSA evaluates and manages risks to the transportation modes for which it is responsible arising from international or domestic terrorists, insiders, or other adversaries.
- TSA considers the interconnected and interdependent nature of the physical, human, and cyber components of the transportation infrastructure when assessing risks and response plans.
- TSA recognizes that in order to maximize the value provided to the Nation, a systems approach to risk management is necessary to balance security effectiveness with operational efficiency, costs, industry vitality, and resource availability.
- TSA evaluates the highest risk scenarios and the effectiveness of security countermeasures as a system using advanced analytical techniques to apply finite resources commensurate with the risk level and to address gaps and weaknesses in current capabilities.

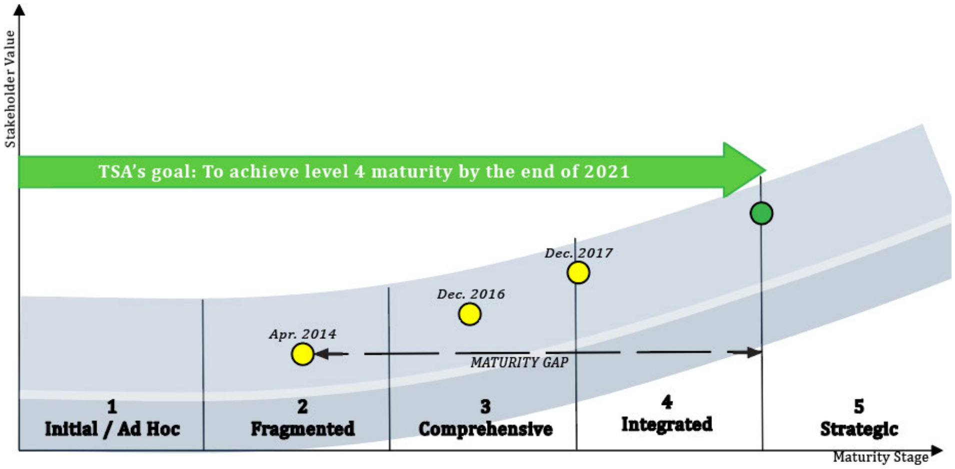
- TSA strikes a balance between countering known risks and hedging against unknown risks by using strategies such as deploying random and unpredictable security countermeasures, enhancing system resiliency, intelligence-driven targeting rules, and effective vetting programs based on sound identity validation and verification processes.
- TSA maintains a flexible capability to focus resources on the basis of real-time threat information.
- TSA takes decisive action to respond to imminent threats with potentially catastrophic consequences, and security effectiveness may take precedence over other considerations.

  TSA evaluates risk levels and implements risk responses and monitoring activities to bring the risk within tolerance without over-controlling non-security related enterprise risks.

ERM MATURITY

TSA began implementation of ERM in 2014 and is currently concentrating on various targeted initiatives to mature and embed robust and consistent risk management practices within the TSA offices in a way that facilitates risk-informed decision making throughout the organization.

Figure 1: TSA ERM Maturity Model



Tinitial / Ad Hoc	Fragmented	Comprehensive	Integrated	Strategic
Risk management activities are ad hoc. No overreaching risk management philosophy or objectives are defined.	Risk management functions independently within business units. Risk types managed are limited to hazard, financial, and compliance.	Risk management is enterprise-wide and encompasses all risks types including strategic and operational. Common standards, tools and techniques implemented. Risk appetite and risk tolerance set for all risks types and strategic risks.	Risks are treated as a portafolio at the enterprise level and are correlated and aggregated across risks types and business units.	Incorporated into capital allocation, product development, etc. Early earning risk indicators. Linkage to performance meassurament iniciatives. Risk modeling scenarios Technology implementation. Industry benchmarking

Consistent standards and well-defined roles and responsibilities are central to a successful ERM program. A first step in creating an ERM program is to understand TSA's current risk management practices across the organization and to determine how TSA aligns to our Capability Maturity Model (CMM), designed on industry best practices and tailored to TSA's unique environment. This model contains detailed activities, milestones, attributes and capabilities essential to effective risk management and reflective of levels of maturity: governance, process, people, and technology. Each successive maturity level builds upon the prior level(s) and reflects the evolutionary of ERM from disparate and disconnected efforts, through a comprehensiveness approach to risk management, and leading to a fully integrated risk management program supporting strategic decision-making. These maturity levels define an ordinal scale for evaluating and measuring the maturity of an enterprise's capabilities, and also help to prioritize improvement efforts. The increasing levels of sophistication generally require that leadership dedicate increased time, resources, and executive commitment to implement.

Using the approved CMM, an updated assessment of TSA's maturity level was completed in early-2017 and determined that overall, TSA's risk management practices across the agency were at Level 3 (Comprehensive) maturity. This level is consistent with a mature enterprise that has an established ERM program. TSA has established the goal of reaching Level 4 (Integrated) by the end of 2021. A follow-on review of TSA's ERM activities in mid-2018 showed the agency was making steady progress towards achieving our 2021 goal. The following are recent ERM activities in maturing the program.

During 2018, TSA concentrated on developing and implementing a new process to meet the new A-123 requirements, formalized risk reporting tools, and began to better promote ERM at TSA by:

- Developing a methodology and completing three test cases for the alignment of enterprise risk responses with internal controls in support of the A-123 requirement,
- Developing risk reporting tools used to support decision making,
- Beginning to develop Key Risk Indicators (KRI) with risk owners,
- Developing a process for risk to be a required consideration and decision criteria for all budget decisions at the business unit and enterprise levels,
- Implementing a ERM communications strategy.

During 2017, TSA concentrated on developing common frameworks and updated processes to better coordinate risk management activities at TSA by:

- Developing a new format for the TSA Risk Register,
- Determining TSA's prioritized enterprise risks with the ERSC,
- Gathering additional data from risk owners on enterprise risks,
- Finalizing a new process for receiving enterprise risk updates,
- Working with Finance and Administration to formalize risk as a consideration for budget decisions,
- Completing TSA's risk profile submitted to OMB in support of the new A-123 requirements.

Past ERM Maturity Activities (2014-16)

During 2016, TSA concentrated on operating, sustaining, and maturing ERM capabilities by:

- Implementing risk response plans and tracking progress against risk objectives for Programs,
- Performing dynamic monitoring of KRIs to assess potential for risk events in line with established risk tolerance thresholds,
- Performing on-going risk reporting to inform decision making at the enterprise level
- Building further linkages between ERM, internal controls, and resource allocation processes to embed risk-based decision-making throughout the

organization,

- Determining hardware, software, and environment requirements for ERM IT support system and preparing for installation,
- Continuing to build organizational capacity through external training, disseminating leading research and practices, and professional networking and knowledge-sharing (TSA Risk Community of Interest),
- Implementing ERM training for appropriate staff and collaborating with other TSA offices to embed targeted risk management techniques and decision-making tools into existing train.

During 2014 and 2015, efforts centered on establishing the ERM infrastructure and capabilities. Specifically, TSA:

- Approved ERM policy and defined the ERM organizational structure and policy manual,
- Established risk appetite statements and developed risk tolerance thresholds in line with risk appetite,
- Defined enterprise risk assessment criteria,
- Developed risk reporting process and templates,
- Amended performance measures to embed risk management responsibilities and goals,
- Defined high-level requirements for ERM information system.

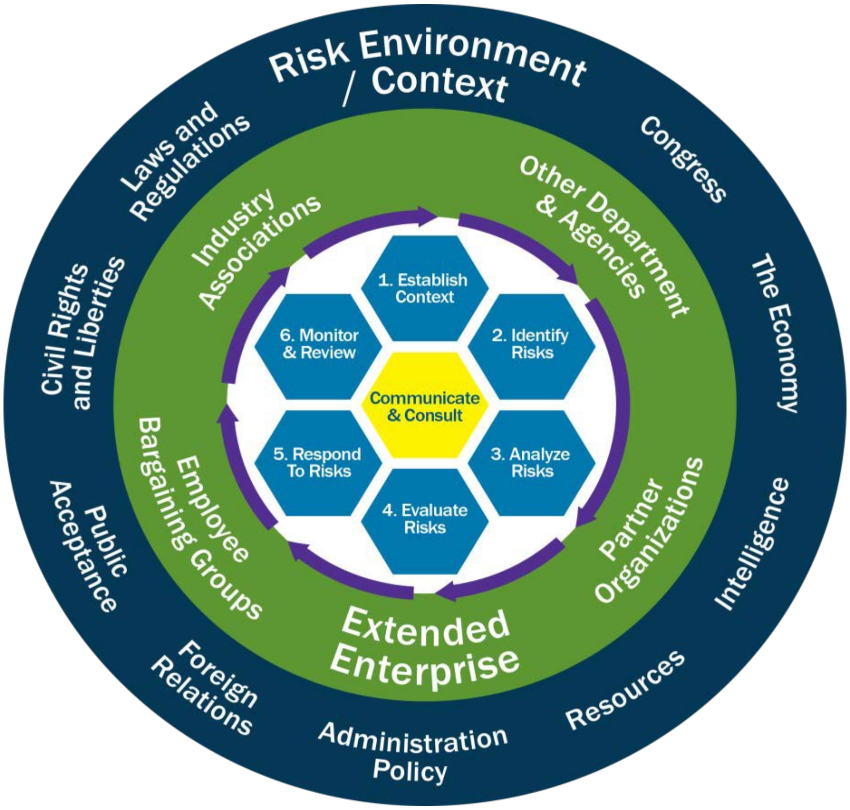
Building on this ERM foundation, TSA then focused on implementing the ERM process across the Agency through various initiatives as:

- Performing enterprise risk identification through multi-disciplinary stakeholder working groups,
- Assessing enterprise risks using quantitative and qualitative methods,
- Prioritizing risks, assign risk owners, and develop response plans aligned to TSA risk tolerance thresholds,
- Finalizing requirements and perform ERM IT support system selection,
- Developing and disseminating a risk culture survey with action plans based on results,
- Developing and implementing risk management training for all TSA employees.

ERM PROCESS FRAMEWORK

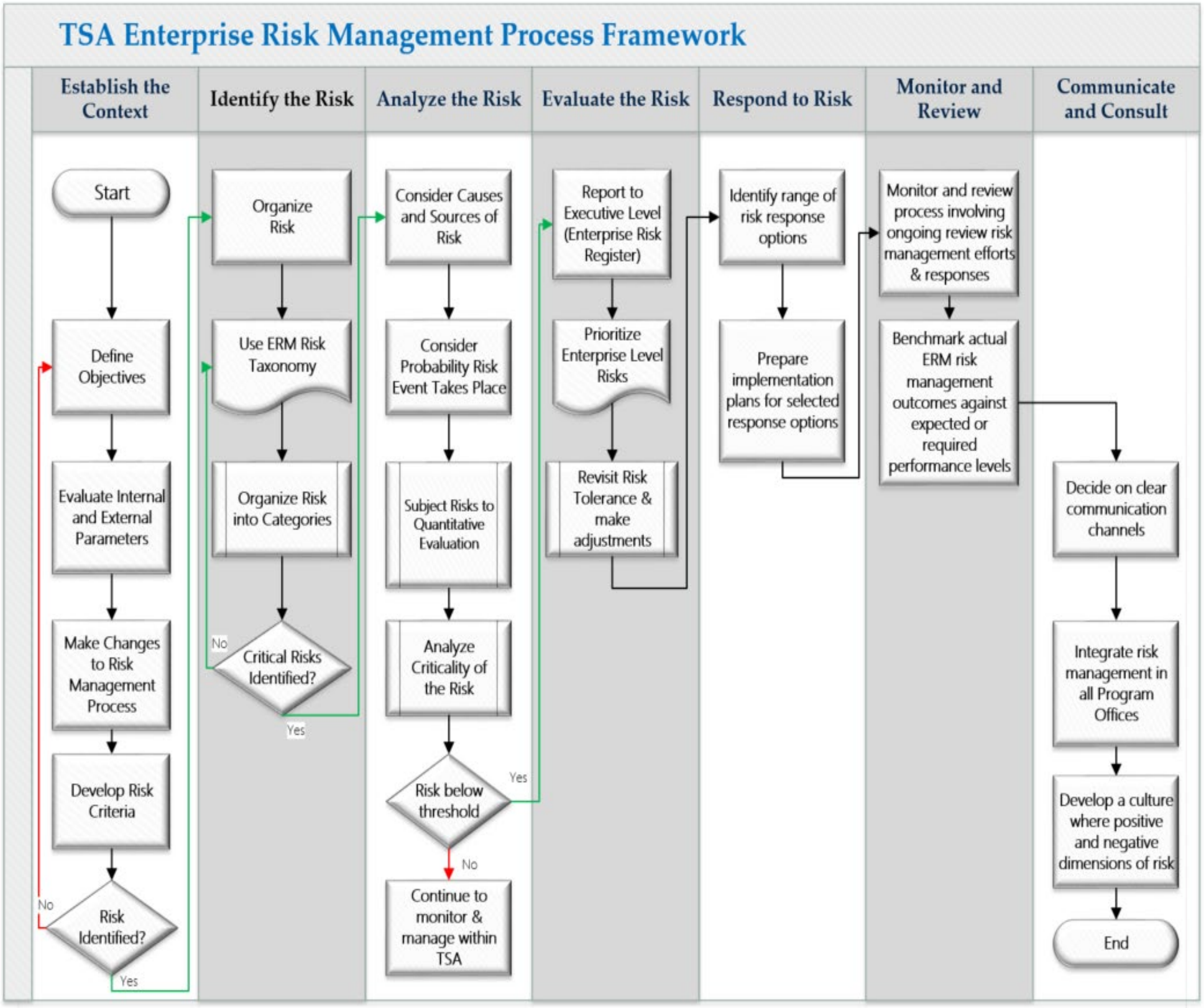
Managing risk is not linear and does not take place in a vacuum. Rather, effective risk management represents the balancing of a number of interwoven internal and external factors which shape the risk environment and decision context, and limit risk response alternatives. Furthermore, specific risks cannot be addressed in isolation from each other; the management of one risk may have an impact on another, or management actions which are effective in controlling more than one risk simultaneously may be achievable.

Figure 2: TSA Enterprise Risk Management Process[1]



[1] 1 Beers, R., (2011), Risk Management Fundamentals, Homeland Security Risk Management Doctrine, U.S. Department of Homeland Security, Washington, D.C., April 2011, p. 15

Figure 3: TSA Enterprise Risk Management Process Framework


TSA Enterprise Risk Management Process Framework
Establish the Context
Identify the Risk
Analyze the Risk
Evaluate the Risk
Respond to Risk
Monitor and Review
Communicate and Consult
Start
Define Objectives
Evaluate Internal and External Parameters
Make Changes to Risk Management Process
Develop Risk Criteria
Risk Identified?
No
Yes
Organize Risk
Use ERM Risk Taxonomy
Organize Risk into Categories
Critical Risks Identified?
No
Yes
Consider Causes and Sources of Risk
Consider Probability Risk Event Takes Place
Subject Risks to Quantitative Evaluation
Analyze Criticality of the Risk
Risk below threshold
Yes
No
Continue to monitor & manage within TSA
Report to Executive Level (Enterprise Risk Register)
Prioritize Enterprise Level Risks
Revisit Risk Tolerance & make adjustments
Identify range of risk response options
Prepare implementation plans for selected response options
Monitor and review process involving ongoing review risk management efforts & responses
Benchmark actual ERM risk management outcomes against expected or required performance levels
Decide on clear communication channels
Integrate risk management in all Program Offices
Develop a culture where positive and negative dimensions of risk
End

The ERM process framework (see Appendix 1) and depicted below (is being implemented by TSA. It is closely aligned with the DHS Risk Management Process[1] and incorporates elements from the International Standards Organization (ISO) 31000:2009 Risk Management — Principles and Guidelines and the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management Integrated Framework (2004). By necessity, the model represents the risk management process as discrete sub-elements for illustrative purposes, but in reality they blend together. In addition, the particular stage in the process which one may be at for any particular risk will not necessarily be the same for all risks.

This model also illustrates how the core risk management process is not isolated, but takes place in a context; and, how certain key elements have to be given careful consideration in order for the overall process to generate the outcomes desired from risk management. Risk management must function in an environment in which risk appetite has been defined. The concept of risk appetite (how much risk is tolerable and justifiable) should be regarded as an "overlay" across the whole of this model.

This risk management process provides a logical and systematic method for establishing the context for risks, as well as identifying, analyzing, evaluating, responding to, monitoring, and communicating them in a way that will allow TSA to make decisions and respond timely to risks and opportunities as they arise. This approach promotes comparability and a shared understanding of information and analysis in the decision process and facilitates a better risk management structure and risk-informed decision making. A high level description of each process step within the ERM framework is presented below.

Establish the Context

The *Establish the Context* process step involves understanding and articulating the internal and external environment of the organization. During this step, TSA defines its objectives, evaluates the external and internal parameters to be taken into account when managing risk, makes changes to the risk management process, and develops risk criteria.

Identify Risks

During the *Identify Risks* process step, TSA seeks to identify enterprise-level risks to be managed using a structured, systematic process called the Enterprise Risk Register. This process specifies what risks can occur, as well as where, when, why, and how they may occur. The list of risks identified through this process is preliminary and subject to further qualification and refinement as part of the following *Analyze Risks* process. The *Identify Risks* process captures risks using TSA's enterprise risk taxonomy and then progressively narrows the list to the most critical using first qualitative and then quantitative techniques in the *Analyze Risks* process.

Analyze Risks

The *Analyze Risks* process involves consideration of the causes and sources of risk, the probability that the risk event will occur, their positive or negative consequences and magnitude, and the likelihood that those consequences may occur. Risk analysis provides the basis for evaluation and decisions regarding risk response or treatment. Each risk identified during the *Identify Risks* process is subjected to a qualitative evaluation of its likelihood and impacts. The list of risks is then narrowed and refined based on the criticality of the risk. Those risks falling below a defined threshold may continue to be monitored and managed within TSA, but will not be reported at the executive level as part of the Enterprise Risk Register.

Evaluate Risks

The *Evaluate Risks* process uses the qualitative risk analysis generated in the preceding *Analyze Risk* process to rank and prioritize enterprise level risks. By prioritizing the enterprise-level risks, TSA leadership can respond as appropriate with strategic allocation of resources in the *Respond to Risks* process. Usually, risk managers find that responding to a few critical risks results in dramatic reductions in residual risk. During *Evaluate Risks*, TSA leadership should revisit the documented risk tolerances in light of their overall risk portfolio and make adjustments.

Respond to Risks

The *Respond to Risks* process involves identifying and assessing the range of risk response options and preparing implementation plans for selected response options. Responding to risks includes both the seizing of opportunities to achieve mission success as well as efforts to minimize the adverse impacts of risk. Using a prioritized list of quantified risks requiring response options from the *Evaluate Risks* process, TSA leadership can make informed strategic decisions about how to allocate resources to programs and projects reflected in the enterprise risk register.

Monitor and Review

The *Monitor and Review* process involves ongoing review risk management efforts and response strategies to ensure they remain relevant and effective. Factors that may affect the likelihood and consequences of an outcome may change over time, as may the factors that affect the suitability or cost of the selected response options. It is therefore necessary to repeat the risk management cycle regularly. *Monitor and Review* also involves benchmarking actual ERM risk management outcomes against expected or required performance levels.

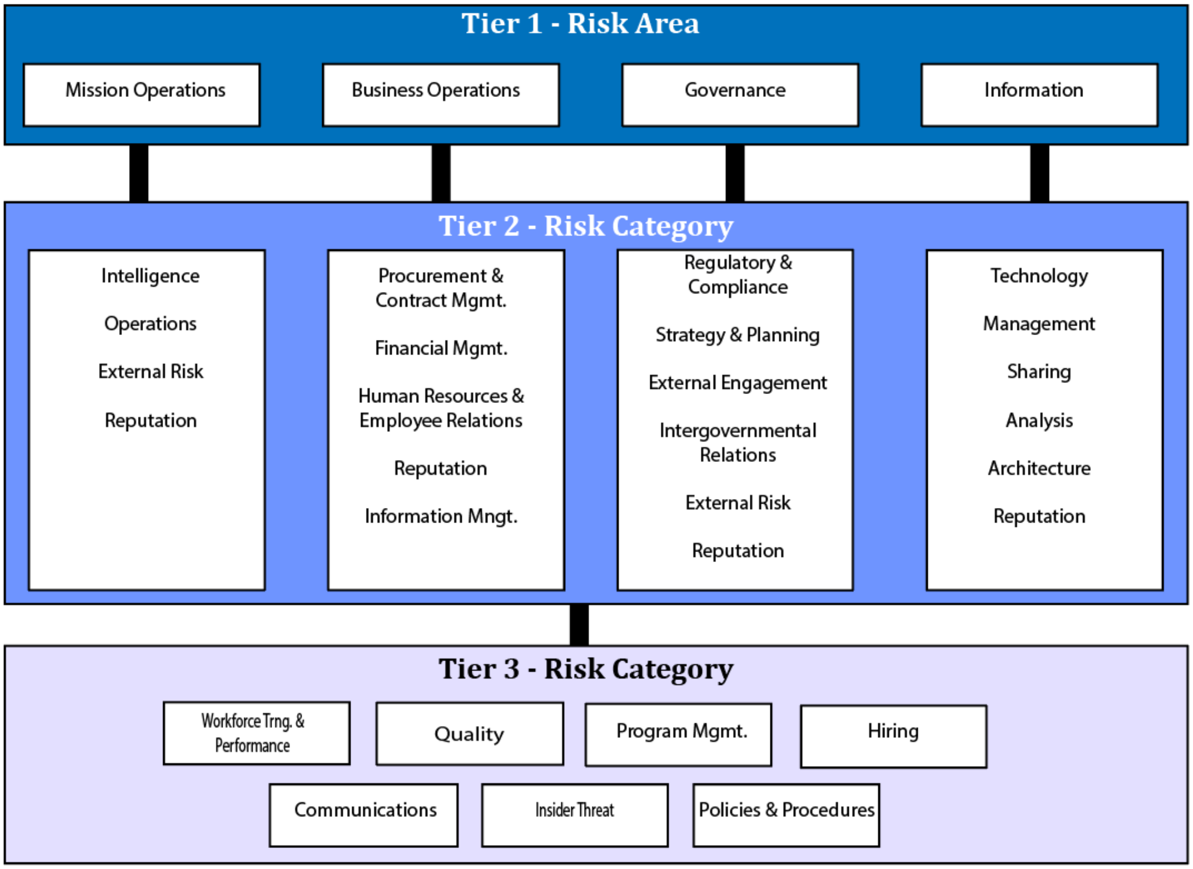
Communicate and Consult

Communication and Consultation process leverages existing channels to escalate risk information to senior leadership in order to obtain their feedback and guidance as appropriate. Clear communication channels are essential to fully integrating risk management in all programs and to developing a culture where positive and negative dimensions of risk are recognized and valued.
TSA office

ERM RISK TAXONOMY

The ERM Risk Taxonomy (see Appendix 1) organizes risk into categories to promote consistent identification, assessment, measurement, and monitoring of risks across the organization. Using a common and consistent risk taxonomy across the entire organization enables TSA to determine the relationships between various risks in a manner that allows improved assessment of the overall impact to the organization. Figure 3 illustrates TSA's ERM risk taxonomy, including 3 tiers of risk categories. The four tables that follow further define the Tier 2 risk categories within each Tier 1 risk area. Taxonomy tiers are intended to provide increasing levels of detail for a specific risk, and do not denote levels of importance.

Figure 4: Risk Taxonomy



ERM ROLES AND RESPONSIBILITIES

TSA Administrator

The TSA Administrator maintains ultimate accountability for the management of the agency's risks, including issuing directives for their management. The Administrator also authorizes and owns the TSA ERM Policy and issues final approval of the ERM risk appetite statements.

Executive Assistant Administrators (EAAs):

EAAs, who comprise TSA's Senior Leadership Team (SLT), serve as ultimate risk owners in accordance with the ERSC Charter. TSA offices will adopt and follow the ERM framework and the TSA ERM Policy and participate in enterprise-wide risk management efforts and perform risk management activities within their individual office. EAAs are responsible for implementing consistent risk management practices in alignment with this policy, including but not limited to the following:

- Escalating risks to SP&I for consideration as additions to the TSA Risk Register;
- Implementing TSA office-level processes to identify systemic security vulnerabilities, in support of the Centralized Security Vulnerability Management Process;
- Integrating considerations of risk into TSA offices' resource allocation decision-making and strategic planning processes; and
- Aligning management control techniques to TSA office risks and ensuring these techniques are integrated into the Management Control Objective Plan program.

It is also the responsibility of the TSA offices to disaggregate the enterprise level risk appetite statements into TSA office specific risk limits, where applicable, and develop and monitor Key Performance Indicators (KPIs) and KRIs. TSA offices and EAAs will also assist the ERM Team by nominating Subject Matter Experts (SMEs) to serve on risk assessment teams during the risk identification, analysis, and evaluation processes. EAAs will serve as Risk Owners for assigned enterprise level risks and will be responsible for the implementation and monitoring of risk response strategies and associated KRIs.

Executive Risk Steering Committee (ERSC)

The role of the ERSC, chaired by the CRO and composed of all Assistant Administrators (AAs), is to oversee the development and implementation of processes used to analyze, prioritize, and address risks across TSA. These risks include terrorism threats facing the entire transportation sector, along with non-operational risks that could impede TSA's ability to achieve its strategic objectives. The ERSC is broadly responsible for ensuring that risks are managed to create value for the Nation and in a manner consistent with established risk appetite and risk tolerances levels. Specific duties and responsibilities are depicted in the ERSC Charter attached as Appendix 1 to this manual.

Strategy, Policy Coordination and Innovation (SP&I)

The Strategy, Policy Coordination and Innovation (SP&I) develops, coordinates, and synchronizes strategic-level strategies, plans, performance measures, risk, policies, and innovation activities to meet the Administrator's intent and priorities while harnessing new opportunities to advance transportation security. Enterprise Performance and Risk (EPR) branch, which is TSA's lead in ERM, is located within SP&I.

Enterprise Performance and Risk (EPR)

The Enterprise Performance and Risk (EPR) branch is the lead TSA entity for all enterprise risk matters that could impact TSA's ability to perform its mission. EPR is responsible for the design, development, and implementation of the ERM program at TSA and ensuring TSA is in compliance with federal risk management guidance, such as OMB Circular A-123. EPR, with the support of the Risk IPT, ERSC and risk owners, conducts regular enterprise risk assessments of TSA business processes or programs regularly and oversees the identification, assessment, prioritization, response, and monitoring of enterprise risks, which includes the development of enterprise level Key Risk Indicators (KRIs). In addition, EPR works with Inspections (INS) on the implementation and monitoring of the TSA-wide Security Vulnerability Management Process (SVMP). EPR also supports Finance and Administration (CFO) with the yearly RAP process by providing advisory support on risk.

TSA Office ERM Liaisons

TSA office ERM Liaisons are designated individuals within each TSA office that serve as the primary representative to the ERM Team. ERM Liaisons are responsible for communicating with the ERM Team and supporting TSA office risk owners throughout the ERM process, as necessary. They also serve as an advisory body that shares information and provides subject matter expertise to support ERM program activities, such as the identification, validation, and assessment of enterprise risks.

Risk Analysis Integrated Project Team (IPT)

Risk Analysis IPTs are comprised of cross-functional subject matter experts (SMEs) that are responsible for assessing a defined enterprise risk to identify cross-functional root causes and consequences. IPT members will assist the ERM Team and Risk Owners to assess enterprise risks, identify risk response options, perform cost- benefit analysis, identify Key Risk Indicators (KRIs), and develop recommendations for risk response and monitoring plans for enterprise risks.

TSA Employees

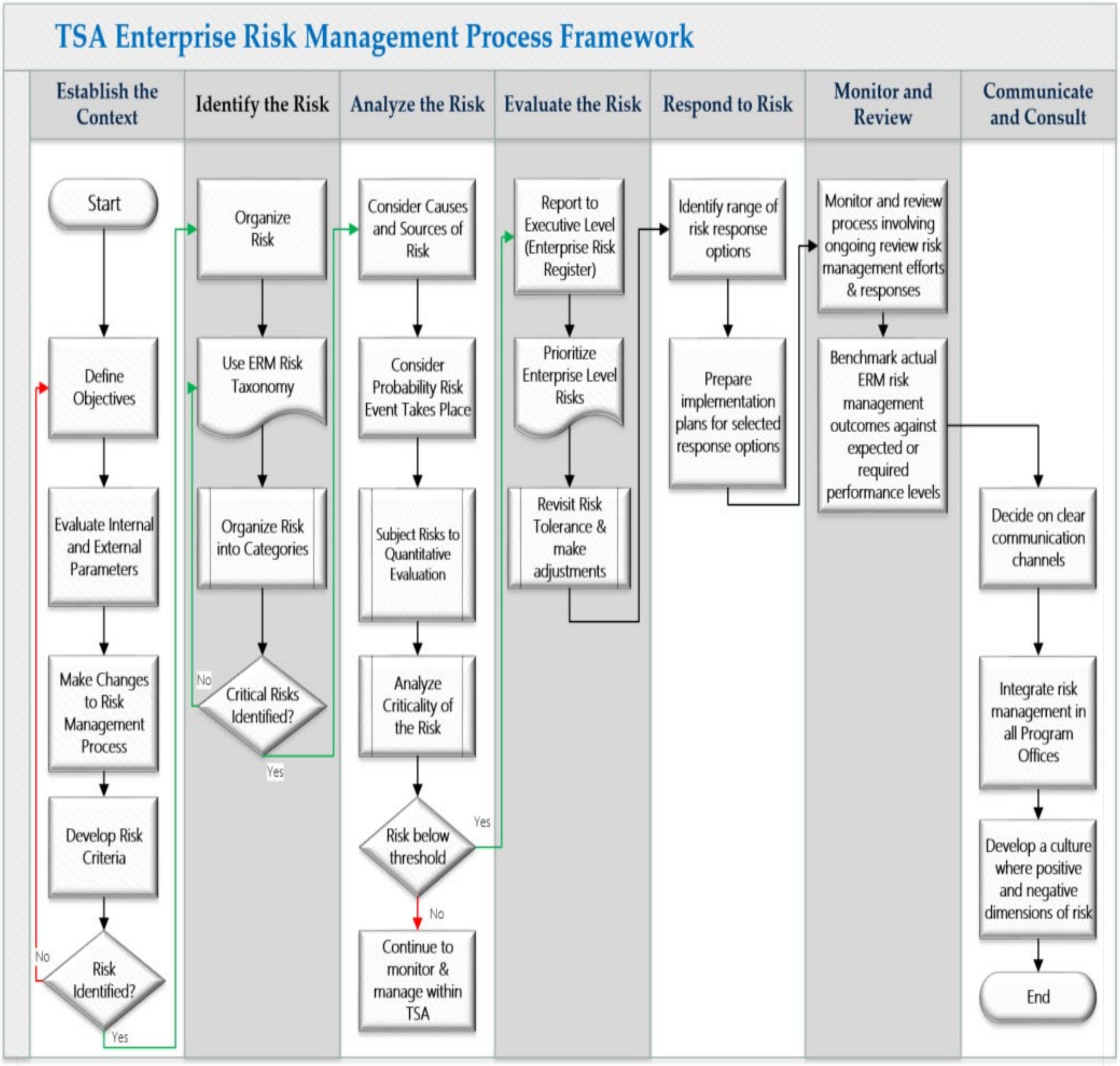
Effective ERM programs require both leadership and employees to actively own and commit to the success of the program. As such, it is the responsibility of all TSA employees to complete required risk management training which is designed to enable every TSA employee to integrate risk-based decision-making principles into their daily work.

Related Laws, Regulations, and Policy Exceptions

ERM policies, procedures, and activities must comply with Government Statutes and Laws as well as requirements dictated by the U.S. Congress, U.S. Department of Homeland

Security (DHS), U.S. Government Accountability Office (GAO), and other relevant stakeholders. Any exception to this policy must be documented in writing and approved by the AA of the TSA office and forwarded to the CRO for notification, review, and approval. The Enterprise Performance and Risk (EPR) branch of SP&I will track policy exceptions and report this status to the ERSC. Additionally, policy exceptions must be reviewed and approved by TSA’s SLT.

APPENDIX 1: TSA ENTERPRISE RISK MANAGEMENT PROCESS FRAMEWORK


TSA Enterprise Risk Management Process Framework
Establish the Context
Identify the Risk
Analyze the Risk
Evaluate the Risk
Respond to Risk
Monitor and Review
Communicate and Consult
Start
Define Objectives
Evaluate Internal and External Parameters
Make Changes to Risk Management Process
Develop Risk Criteria
Risk Identified?
No
Yes
Organize Risk
Use ERM Risk Taxonomy
Organize Risk into Categories
Critical Risks Identified?
No
Yes
Consider Causes and Sources of Risk
Consider Probability Risk Event Takes Place
Subject Risks to Quantitative Evaluation
Analyze Criticality of the Risk
Risk below threshold
Yes
No
Continue to monitor & manage within TSA
Report to Executive Level (Enterprise Risk Register)
Prioritize Enterprise Level Risks
Revisit Risk Tolerance & make adjustments
Identify range of risk response options
Prepare implementation plans for selected response options
Monitor and review process involving ongoing review risk management efforts & responses
Benchmark actual ERM risk management outcomes against expected or required performance levels
Decide on clear communication channels
Integrate risk management in all Program Offices
Develop a culture where positive and negative dimensions of risk
End

APPENDIX 2: ENTERPRISE RISK MANAGEMENT POLICY STATEMENT

The Nation's transportation systems are vital to the economic health and security of our country. Protecting the Nation's transportation systems to ensure the freedom of movement for legitimate travelers and commerce is the mission of the Transportation Security Administration (TSA).
Implementing effective risk management principles in all modes of transportation and across all functions and programs within TSA is essential to successfully accomplishing this mission.

Our risk-management approach must support our ability to identify, analyze, and appropriately respond to risks across the full spectrum of TSA activities, and leverage the capabilities of our partners to address gaps, reduce vulnerabilities, and mitigate threats. Under the direction of the Chief Risk Officer, working with the Executive Risk Steering Committee, TSA will continue to develop and implement Enterprise Risk Management as the framework for risk management activities across the organization. Through our Enterprise Risk Management program, we will:

- Provide a structured, disciplined, and consistent approach to identifying, reporting assessing, and monitoring risk aligned with U.S. Department of Homeland Security guidance.
- Identify, assess, and manage enterprise risks that threaten TSA's achievement of our mission or impede accomplishing our long-term goals and objectives.
- Ensure that enterprise and program risks are managed consistent with defined risk appetite and established risk-tolerance levels.
- Align our strategy, programs, processes, people, technology, information, and budget to maximize the value TSA provides to the Nation.
- Maintain a cross-organizational strategic focus that allows TSA to adapt to changes in risk; rapidly field new operating concepts performance standards and capabilities; and invest appropriately in our workforce.
- Provide greater transparency into risks by improving our understanding of interactions and relationships between risks, thereby improving risk-based decision making.
- Establish clear accountability and ownership of risk.

APPENDIX 3: ERSC CHARTER

TRANSPORTATION SECURITY ADMINISTRATION EXECUTIVE RISK STEERING COMMITTEE CHARTER AUGUST 2015

PURPOSE

The purpose of this charter is to establish the duties, responsibilities, and membership of the Transportation Security Administration's (TSA) Executive Risk Steering Committee (ERSC).

This document supersedes the March 2014 ERSC Charter.

BACKGROUND

Applying effective risk management principles in all modes of transportation and across all functions and programs within TSA is essential to successfully accomplishing the TSA mission. The growth in the number of tools and methodologies used to assess risk, and increased emphasis on risk management within TSA and across the U.S. Department of Homeland Security (DHS), necessitates the establishment of an executive-level risk governance structure.

The ERSC fulfills a critical executive governance role for TSA, with overarching responsibility for overseeing the development and implementation of Enterprise Risk Management (ERM) across the organization, and for managing risk at an enterprise level. Through TSA's ERM program, the ERSC ensures consistent application of processes necessary to identify, analyze, prioritize, and respond to risk throughout TSA at both the enterprise level and individual program level, ensuring clear accountability and ownership of risk. At the enterprise level, these risks encompass TSA's ability to successfully combat terrorism threats to the Nation's transportation systems, as well as non-operational risks that could impede TSA's ability to achieve its transportation security mission or strategic objectives.

DUTIES AND RESPONSIBILITIES

As a collective governance body, the ERSC is broadly responsible for establishing risk policies; identifying enterprise level risk to be placed on the enterprise risk register; approving mitigation strategies and controls for these risks; assigning a lead executive with responsibility for coordinating and reporting risks; reviewing the status and effect of approved mitigation strategies; approving and directing additional response actions when required; and integrating risk with TSA's strategy, budget planning, and resource-allocation decisions. These activities ensure that significant risks to TSA are effectively managed consistent with TSA's established risk appetite and risk tolerance levels in order to maximize the value TSA provides to the Nation through our program and activities. The primary functions of the ERSC are to assist the Administrator and Deputy Administrator in oversight of key Agency risks through the following responsibilities:

- Developing, implementing, and applying TSA's ERM Policy;
- Ensuring the effective operation of the ERM Framework and setting the tone for risk management throughout TSA;

- Recommending the risk appetite and associated risk-tolerance level for each major
- category of risk associated with TSA's strategic objectives;
- Setting the risk-based security and risk-management strategies for TSA and providing strategic oversight;
- Identifying, prioritizing, and monitoring the most significant enterprise risks reflected
- through the strategic risk register and ensuring appropriate risk response and mitigation plans are working to achieve desired outcomes;
- Identifying, mitigating, and monitoring the top strategic enterprise risks reflected on the Agency's Enterprise Risk Register;
- Sponsoring and providing oversight, direction, and review for working groups and assessment teams tasked with analyzing specific risks and/or related policies; and,
- Aligning risk with TSA's strategy, budget planning, and resource allocation decisions.

As TSA executives, ERSC members are responsible for managing risks within their respective TSA offices. However, when participating as a member of the ERSC, they have an obligation to consider risk management from an Agency-wide perspective. Specified duties of ERSC members include:

- Attending ERSC meetings in person or appointing a designated alternate empowered to make decisions. Prior approval from the Chair is needed should this person be below the level of Deputy Assistant Administrator.
- Appointing knowledgeable and empowered representatives and a designated alternate to participate on working groups and assessment teams established by the ERSC.
- Elevating major risk-related decisions to the full ERSC as necessary.
- Reviewing read-ahead materials prior to the meeting.
- Facilitating ERM-related communications within their respective TSA offices.

ORGANIZATION

ERSC membership includes all Assistant Administrators as the scope of TSA's risk management efforts is enterprise-wide. Deputy Assistant Administrators may attend ERSC meeting as a non-voting participant and will serve as the alternate to their Assistant Administrator. Other subject matter expe1ts and briefers will participate in specific meetings as deemed necessary when requested by an ERSC member and approved by the Chief Risk Officer.

The Chief Risk Officer will serve as the Chair for all ERSC meetings. When the Chief Risk Officer is unavailable, an Assistant Administrator will be designated to lead the ERSC meeting. A project management staff suppo1ts the Chair in preparing for and conducting the ERSC meetings. As required, the ERSC oversees the progress of working groups that consist of executive- and staff-level participants. Working groups develop detailed plans defining milestones and key deliverables that meet requirements and tasks from the ERSC.

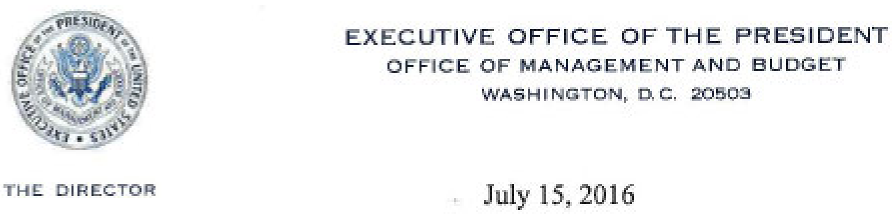
At a minimum, the ERSC shall meet in person on a monthly basis. Additionally, the Chair may schedule ad hoc meetings at his or her discretion. Each member shall have one vote. The quorum for decision-making is more than 50 percent of the members or designated alternatives present. A simple majority of the attendees is required to bring a decision forward to the Administrator and Deputy Administrator. Unanimous concurrence is not required, and contrary opinions will also be brought forward to the Administrator and Deputy Administrator for their consideration in making a final decision.

APPROVAL

Peter V. Neffenger
Administrator

APPENDIX 4: OMB CIRCULAR NO. A-123

On July 15, 2016, the OMB updated its Circular No. A-123 to modernize existing efforts by encouraging Agencies to implement and coordinate ERM capability with strategic planning and internal controls. The Transportation Security Administration's (TSA) integration of Enterprise Risk Management (ERM) and internal controls is an ambitious effort. Strategy, Policy Coordination and Innovation (SP&I) developed a framework to being to align Enterprise Risks with internal controls and explored an avenue to align budget with this data. The framework was then piloted with three (3) test cases of Enterprise risks to probe assumptions and document specific findings and recommendations. The full implementation of the A-123 ERM & Internal Control Integration Process, with the testing of efficiency and effectiveness and resource alignment, is an iterative process that will include the careful review and assessment of TSA's Enterprise Risks and internal controls.



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

July 15, 2016

M-16-17

MEMORANDUM TO THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shaun Donovan

Director

SUBJECT: OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control

The Administration has emphasized the importance of having appropriate risk management processes and systems to identify challenges early, to bring them to the attention of Agency leadership, and to develop solutions. To that end, the Office of Management and Budget (OMB) is updating this Circular to ensure Federal managers are effectively managing risks an Agency faces toward achieving its strategic objectives and arising from its activities and operations. These expanded responsibilities reinforce the purposes of the Federal Managers' Financial Integrity Act (FMFIA) and the Government Performance and Results Act Modernization Act (GPRAMA), and support the Administration's commitment to improve the efficiency and effectiveness of Government.

Since 1981, OMB Circular No. A-123 (A-123) and FMFIA have been at the center of Federal requirements to improve accountability in Federal programs and operations. Over the years, government operations have changed dramatically, becoming increasingly complex and driven by changes in technology. At the same time, resources are constrained and stakeholders expect greater program integrity, efficiency and transparency into government operations.

The policy changes in this Circular modernize existing efforts by requiring agencies to implement an Enterprise Risk Management (ERM) capability coordinated with the strategic planning and strategic review process established by GPRAMA, and the internal control processes required by FMFIA and Government Accountability Office (GAO)'s Green Book. This integrated governance structure will improve mission delivery, reduce costs, and focus corrective actions towards key risks. Implementation of this policy will engage all agency management, beyond the traditional ownership of OMB Circular No. A-123 by the Chief Financial Officer community. In particular, it will require leadership from the agency Chief Operating Officer and Performance Improvement Officer, and close collaboration across all agency mission and mission-support functions.

Successful implementation of this Circular requires Agencies to establish and foster an open, transparent culture that encourages people to communicate information about potential risks and other concerns with their superiors without fear of retaliation or blame. Similarly, agency managers, Inspectors General (IG) and other auditors should establish a new set of parameters encouraging the free flow of information about agency risk points and corrective measure adoption. An open and transparent culture results in the earlier identification of risk, allowing the opportunity to develop a collaborative response, ultimately leading to a more resilient government.

This revision of the Circular has gone through an extensive deliberative process with Agencies and their IG teams, and including consultation with the GAO and many outside groups who seek more efficient and effective delivery of governmental services. This revised Circular is effective for Fiscal Year (FY) 2016 and supersedes all previous versions. Appendices A, B, C, and D of OMB Circular No. A-123 remain in effect. Updates to the GAO green book are effective for FY 2016. ERM implementation requirements are effective for FY 2017. OMB plans to work closely with the President's Management Council, Executive Councils, and the Council of lnspectors General on Integrity and Efficiency (CIGIE) to provide further implementation guidance.

U.S. Department of Homeland Security
Office of Intelligence and Analysis
601 S. 12th Street
Arlington, VA 20598

Transportation
Security
Administration

7 May 2019

INFORMATION

MEMORANDUM FOR: [redacted]
Investigator
TSA Investigations

FROM: [redacted]
Deputy Director, Threat Analysis
Intelligence and Analysis

SUBJECT: Research Related to OSC File Nos. DI-18-5205 and DI-19-0778

Purpose

To inform you of the results of our intelligence research related to Office of Special Counsel's Files DI-18-5205 and DI-19-0778.

Background

On 12 April 2019, you asked if there was any threat intelligence relating to allegations that TSA had failed to properly protect flight crews and the public from potential opioid attacks and that TSA had failed to prevent significant security breaches because of its policy exempting religious food trucks from airport inspections.

Discussion

We tasked intelligence analysts to look into these two areas, and they found nothing to support the idea that terrorists have considered or are considering either these two methods (opioids or food trucks) of attack. We did not ask analysts to review TSA operational reporting to look for incidents involving either opioid attacks or food trucks, nor did we ask them to research into TSA policy regarding either of these two issues.

Transportation
Security
Administration

OFFICE OF THE CHIEF RISK OFFICER

TSA MANAGEMENT DIRECTIVE No. 100.8
Enterprise Risk Management

To enhance mission performance, TSA is committed to promoting a culture founded on its values of Integrity, Innovation and Team Spirit.

1. **PURPOSE:** This directive provides TSA policy and procedures for enterprise risk management (ERM).

2. **SCOPE:** This directive applies to all TSA Program Offices and risk management staff that support the development and implementation of ERM at TSA.

3. **AUTHORITIES:** Office of Management and Budget (OMB) Circular A-11 Sections 270.24 – 270.29

4. **DEFINITIONS:**

   A. Enterprise Risk Management (ERM): Comprehensive approach to risk management that engages organizational systems and processes together to improve the quality of decision making for managing risks that may hinder an organization's ability to achieve its objectives.

   B. Executive Risk Steering Committee (ERSC): Governing body that retains overarching responsibility for defining strategy and managing risk at an enterprise level. The ERSC is chaired by the Chief Risk Officer (CRO) and composed of Assistant Administrators (AAs) from the Offices of Acquisition, Finance and Administration, Human Capital, Information Technology, Global Strategies, Intelligence and Analysis, Law Enforcement/Federal Air Marshal Service, Security Capabilities, Security Operations, and Security Policy and Industry Engagement.

   C. Key Risk Indicator (KRI): Measures that provide an early warning system that a risk is occurring or has occurred.

   D. Risk: Potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and associated consequences.

   E. Risk Appetite: Amount and type of risk that an organization is willing to pursue or retain.

   F. Risk Owner: Person or entity with the accountability and authority to manage a risk.

   G. Issue: An existing event or condition that an organization must address to achieve its mission.

5. **RESPONSIBILITIES:**

   A. The TSA Administrator is responsible for maintaining ultimate accountability for the management of the agency's portfolio of risks across the enterprise, including issuing directives for their management. The Administrator also authorizes and owns the TSA ERM Policy and issues final approval of the ERM risk appetite statements.

B. The Chief Risk Officer (CRO) is responsible for the design, development, and implementation of the ERM program at TSA. The CRO serves as the principal advisor to the Administrator and Deputy Administrator on all risk matters that could impact TSA's ability to perform its mission.

C. Assistant Administrators (AAs) are responsible for:

(1) Serving as ultimate risk owners in accordance with the ERSC Charter;

(2) Ensuring that Program Offices adopt and follow the ERM framework and the TSA ERM directive and participate in enterprise-wide risk management efforts within their individual office; and

(3) Implementing consistent risk management practices in alignment with this directive.

NOTE: It will be the responsibility of the Program Offices to disaggregate the enterprise level risk appetite statements into Program Office-specific risk limits, where applicable.

D. The Executive Risk Steering Committee (ERSC) is responsible for:

(1) Overseeing the development and implementation of processes used to analyze, prioritize, and address risks across TSA to include terrorism threats facing the entire transportation sector, along with non-operational risks that could impede TSA's ability to achieve its strategic objectives; and

(2) Ensuring risks are managed to create value for the Nation and in a manner consistent with established risk appetite and risk tolerances levels.

E. The ERM Team is responsible for:

(1) Leading ERM activities under the supervision of the CRO;

(2) Developing and maintaining ERM policies, processes, procedures, tools, and information systems;

(3) Leading efforts to perform enterprise risk identification, assessment, prioritization, reporting, and monitoring; and

(4) Overseeing the process for establishing ERM communication at all levels for gathering data and developing risk reports.

F. TSA Program Office ERM Liaisons are responsible for serving as the primary representative to the ERM Team, communicating with the ERM Team, and supporting Program Office risk owners throughout the ERM process, as necessary.

G. The ERM Working Group (ERMWG) is responsible for:

(1) Sharing information and providing subject matter expertise to support ERM program activities, such as the identification, validation, and assessments of enterprise risks; and

(2) Serving as the primary point of communication between the ERM Team and its members' respective Program Office.

H. Risk Analysis Integrated Project Teams (IPT) are responsible for assessing a defined risk to identify cross-functional root causes and consequences, and coordinate with the ERM Team and risk owners to develop recommendations for risk response and monitoring plans.

6. **POLICY:** The security of the Nation's transportation systems is vital to the economic health and security of America. Ensuring transportation security while promoting the freedom of movement of legitimate travelers and commerce is a critical counter-terrorism mission assigned to TSA. Risk management approach must support TSA's ability to identify, analyze, and appropriately respond to strategic risks across the full spectrum of TSA activities.

A. The Chief Risk Officer, working with the Executive Risk Steering Committee, shall develop and implement ERM as the framework for risk management across the organization. Through ERM, we will:

(1) Provide a structured, disciplined, and consistent approach to assessing risk aligned with U.S. Department of Homeland Security guidance.

(2) Identify strategic risks that threaten TSA's achievement of our long-term objectives and goals, and manage those risks at the enterprise level through the ERSC.

(3) Ensure that risks are managed in a manner that maximizes the value TSA provides to the nation consistent with defined risk appetite and risk tolerance levels.

(4) Align our strategy, process, people, technology, and information to support agile risk management.

(5) Provide greater transparency into risk by improving our understanding of interactions and relationships between risks in support of improved risk-based decision making.

(6) Establish clear accountability and ownership of risk.

B. Risk management is central to TSA's mission, vision, and culture. All employees are expected to adopt the principles of risk management developed through the ERM program, and to apply the standards, tools, and techniques within their assigned responsibilities.

C. TSA creates value by protecting the Nation's transportation systems while enabling the movement of legitimate travelers and goods. TSA seeks practical and cost-effective solutions to effectively reduce the most significant transportation security risks.

D. TSA has different appetites for different risk types expressed in the following statements:

(1) TSA is strongly averse to security risks that could result in catastrophic consequences.

(2) TSA is strongly averse to the compromise of classified information and averse with regard to the compromise of Sensitive Security Information (SSI) and Personally Identifiable Information (PII).

(3) TSA is averse to workforce-related risks pertaining to integrity, performance, health and safety, and regulatory compliance.

(4) TSA is averse to events that could damage its standing and reputation with the traveling public, U.S. Congress, and other federal and industry stakeholders.

(5) TSA is risk neutral with regard to other mission and business operational enterprise risks.

(6) TSA is risk tolerant to programs that enhance the movement of legitimate travelers and goods.

E. TSA makes risk-informed decisions to achieve its mission within the parameters of its risk appetite:

(1) TSA evaluates and manages risks to the five transportation modes for which it is responsible arising from international terrorists, homegrown violent extremists, insiders, or other adversaries.

(2) TSA considers the interconnected and interdependent nature of the physical, human, and cyber components of the transportation infrastructure when assessing risks and response plans.

(3) TSA recognizes the need to balance security effectiveness with operational efficiency, cost, industry vitality, and passenger satisfaction by taking a systems approach to risk management.

(4) TSA evaluates the highest risk scenarios and the effectiveness of layered security counter-measures using advanced computational techniques to apply finite resources commensurate with the risk level.

(5) TSA strikes a balance between countering known risks and hedging against unknown risks by using strategies such as deploying random security countermeasures and enhancing system resiliency.

(6) TSA maintains a flexible capability to focus resources on the basis of real-time threat information.

(7) TSA takes decisive action to respond to imminent threats with potentially catastrophic consequences and security effectiveness may take precedence over other considerations.

(8) TSA evaluates risk levels and implements risk responses and monitoring to bring the risk within tolerance without over-controlling non-security-related enterprise risks.

(9) TSA embraces innovation to address adaptive adversaries and changing targets. TSA understands that innovation requires experimentation and balances the need for timely deployment with appropriate testing.

7. PROCEDURES: See TSA ERM Manual.

8. APPROVAL AND EFFECTIVE DATE: This policy is approved and effective the date of signature unless otherwise specified.

APPROVAL

Signed October 22, 2014

_____________________________ ________________
[redacted] Date
Chief Risk Officer

EFFECTIVE

____
Date

Distribution: Senior Management Officials and Business Management Offices (BMOs)
Point-of-Contact: Enterprise Risk Management, [redacted]

Transportation
Security
Administration

Security Vulnerability Management Process (SVMP) Charter

Version 6.4

Revision Date: September 6, 2019

This page is intentionally left blank

OVERVIEW

As security threats against transportation systems evolve, it is vital that the Transportation Security Administration (TSA) has the ability to quickly identify, evaluate, and counter system-wide security vulnerabilities. A security vulnerability is a condition an adversary may take advantage of in order to accomplish a goal. TSA utilizes a framework to assess vulnerabilities across the Agency. This framework includes the process for submitting, evaluating, and tracking the mitigation of vulnerabilities, which will improve TSA's ability to address concerns across the enterprise and better inform the Agency's strategic decision-making, prioritization, and resourcing in the face of numerous security vulnerabilities. It also supports record keeping regarding resource constraints and provides input to the TSA Planning, Programming, Budgeting, Execution and Strategy (PPBE-S) process.

PURPOSE

The purpose of this charter is to formalize procedures and the establish roles and responsibilities related to the Security Vulnerability Management Process (SVMP) within TSA.

GOALS AND OBJECTIVES

The SVMP it the TSA process to manage security risk and to mitigate vulnerabilities that may provide adversaries the opportunity to disrupt the Nation's transportation systems.

The primary goal of the SVMP is to assist in managing security vulnerabilities and track the mitigation of the vulnerabilities. The following process encourages the flow of information and improves understanding regarding security vulnerabilities and mitigation efforts that may impact multiple TSA program offices. It also improves TSA's ability to make prioritized decisions about courses of action to mitigate security vulnerabilities and position TSA to proactively and effectively respond to external stakeholder inquiries *(e.g. Department of Homeland Security (DHS) Headquarters, Congress, DHS Office of the Inspector General (OIG), U.S. Government Accountability Office (GAO))*.

ROLES AND RESPONSIBILITIES

The identification and mitigation of security vulnerabilities that may threaten our transportation infrastructure and systems is a complex process and requires input from multiple stakeholders.

Leadership Council (LC):

The LC serves as the senior forum for cross-functional consideration of the most critical TSA issues. The LC reviews and evaluates TSA objectives, policies, plans, programs, budgets, and studies, and make recommendations to and/or approves same as appropriate. The LC may return issues to the Senior Leadership Team for further study as needed. The Administrator chairs the LC, comprised of the Deputy Administrator, Chief of Staff, and the Executive Assistant Administrators (EAA) for Enterprise Support, Law Enforcement/Federal Air Marshal Service, Operations Support, and Security Operations.

EAAs serve as Executive Sponsors (or "Champions") of individual security vulnerabilities on the SVMP Tracker. Should any item not meet milestones, it is escalated to the LC following the monthly Executive Risk Steering Committee meeting or during the quarterly review sessions.

Executive Risk Steering Committee (ERSC):
Governing body that retains overarching responsibility for developing strategy to mitigate risk at an enterprise level. The Committee is chaired by the Executive Director of Strategy, Policy Coordination, and Innovation office and is composed of Assistant Administrators.

The Committee also retains overarching responsibility regarding management of security vulnerabilities and development/oversight of mitigation action plans. Within 60 days of submission, the ERSC makes the final recommendations regarding formal mitigation action plans, milestones, resourcing, prioritization, target deadlines, and the nomination of Executive Sponsors. It ensures Mitigation Offices are meeting milestones and timeframes and it escalates security vulnerability cases to the LC when additional resources are required or milestones and timeframes are not met. This body consists of Strategy, Policy Coordination, and Innovation (SP&I), Requirements and Capabilities Analysis (RCA), and the specific Assistant Administrators relevant to the associated security vulnerability.

Mitigation Strategy Team (MST):
A collective analytical body composed of subject matter experts from across TSA broadly responsible for evaluating and assessing security vulnerabilities to develop and propose mitigation action plans for ERSC consideration. Within 30 days of submission, the MST meets to determine the context, prioritization, and appropriate security vulnerability mitigation actions; also recommends an EAA as an Executive Sponsor.

The team establishes milestones and timeframes for completing key SVMP steps to reflect the level of effort required. This body consists of representatives from SP&I, RCA, Inspections (INS), Mitigation Offices, and other key supporting offices. The group integrates the Transportation Security Capabilities Analysis Process (TSCAP), the Capability Analysis Report (CAR), and the TSA Enterprise Risk Register during the analysis phase to determine the appropriate vulnerability mitigation actions and prioritization.

Mitigation Offices:
The principal offices responsible for implementing approved security vulnerability mitigation action plans; establishes milestones and timeframes; provides quarterly status updates regarding mitigation action progress and any associated challenges or resource constraints to the MST and Senior Leadership. Works with supporting stakeholders as needed to accomplish the mitigation action plans. Also, assigns a point of contact for each mitigation action on the SVMP Tracker.

Strategy, Policy Coordination, and Innovation (SP&I):
Manages the SVMP process; collects routine updates from Executive Sponsors and the MST; tracks and reports deadlines, milestones, timeframes, and vulnerability mitigation progress; acts as a liaison between program offices and internal TSA stakeholders *(e.g. LC, ERSC, MST, etc.).*

TSA Program Offices:
Submits identified security vulnerabilities to the MST and supports the development and execution of mitigation action plans based on guidance from the ERSC and/or the LC.

GOVERNANCE

Security vulnerabilities may be discovered by many methods, including:

- External Audits
- Comparative Analysis
- Field Evaluation Team
- Covert Red Team Testing
- Joint Vulnerability Assessments
- Modal and Sector Risk Assessments
- Threat Response Group Assessments
- Program Office/Program Assessments
- Employee Misconduct/Fraud Investigations
- Mission, Asset, and System Specific Assessments
- Internal Audits and Management Control Objective Plan

Program offices may identify and submit security vulnerabilities to the MST using a pre-designated SVMP submission form found on the TSA ERM iShare site or via email[1]. The submitting program office coordinates with SP&I to provide a briefing on the submitted security vulnerability to the MST. The MST, in coordination with relevant program offices, will initially analyze the associated risk, propose a mitigation action plan, and recommend an Executive Sponsor within 30 days of submission. The MST briefs the ERSC on the proposed mitigation action plan(s) and the Executive Sponsor recommendations within 60 days of submission. The proposed mitigation action plan(s) and briefing materials will be sent out as read-ahead materials prior to briefing the ERSC members. The ERSC makes a formal recommendation to the LC regarding mitigation actions, milestones, resourcing, prioritization, target deadlines, and assigning an Executive Sponsor.

Once approved by the LC, the Executive Sponsor champions the mitigation action plan to ensure the milestones and deadlines are met as agreed. The MST will track and report on the mitigation actions throughout the process until the item is closed or otherwise resolved. The ERSC will notify the LC when any items do not meet milestones or timelines. Based upon input from the MST, the ERSC will recommend security vulnerability tracking closure to the LC once a mitigation action plan has been completed or the vulnerability has been re-assessed as no longer being a significant concern to TSA. Once a resolution determination has been made, the ERSC recommends a final "close out" of the vulnerability, if approved by the LC, the vulnerability is "closed."

STATUS UPDATES:
SP&I will send a data request to Executive Sponsors the first week of every third month. A response will be required back to SP&I within five days. By the second week of the third month,

[1] If there are difficulties accessing the SVMP submission form, offices can email the SP&I Enterprise Performance and Risk group mailbox at ERM@tsa.dhs.gov.

SP&I will provide a consolidated status update report to the MST. SP&I will also provide (at least) quarterly status reports to the ERSC. The ERSC will review the SVMP Tracker report on a quarterly basis to monitor security vulnerability mitigation progress and will provide updates to the LC. SP&I will provide feedback to the Mitigation Offices within two days of receipt from the ERSC and LC.

VULNERABILITY MANAGEMENT PROCESS TRACKER:
To increase transparency and facilitate in the status tracking of vulnerabilities and mitigation actions, SP&I has created a SVMP Tracker, which is located on the SP&I iShare site.

TSA Security Vulnerability Management Process

02 - Strategy

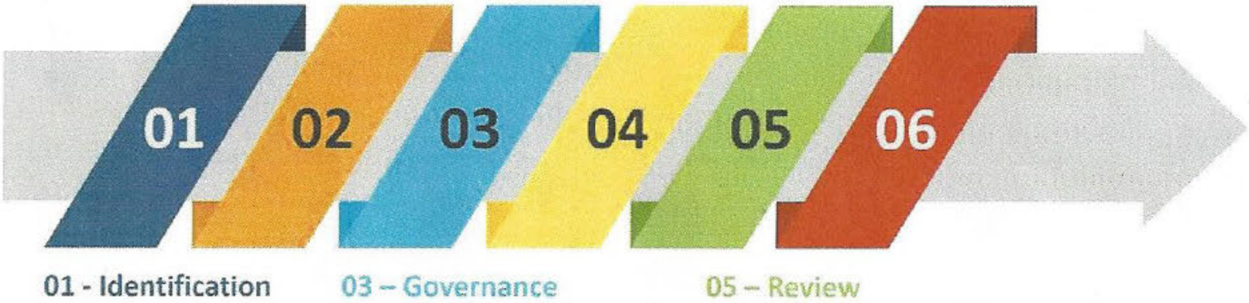
Within **30 days** of submission, the TSA **Mitigation Strategy Team**[1] (MST) meets to determine the context, prioritization, and appropriate security vulnerability mitigation strategy; also recommends an **Executive Sponsor**.

04 - Execution

Once approved by the TSA **LC**, the **Mitigation Offices** take actions to mitigate or resolve the security vulnerability in order to accomplish the milestones and target deadlines established by the **ERSC**.

06 - Resolution

Once resolved and approved by the LC, **Strategy, Policy Coordination, and Innovation** (SP&I) archives the security vulnerability, incorporates data into the **Planning, Programming, Budgeting and Execution** (PPBE) process, and then removes it from the SVMP tracker report.



01 - Identification

Any TSA **Program Office** may submit a security vulnerability for consideration via the standardized TSA intake form.

03 – Governance

Within **60 days** of submission, the TSA **Executive Risk Steering Committee**[2] (ERSC) makes a formal recommendation to the TSA **Leadership Council**[3] (LC) regarding mitigation actions, milestones, resourcing, prioritization, target deadlines, and assigning an **Executive Sponsor**.

05 – Review

The TSA **ERSC** reviews the **Security Vulnerability Management Process** (SVMP) tracker report on a quarterly basis to monitor security vulnerability mitigation progress and provides updates to the TSA LC.

Strategy, Policy Coordination, and Innovation (SP&I)
Enterprise Performance and Risk (EPR)

[1] **SP&I, RCA, INS,** and the **Mitigation Offices**
[2] **Assistant Administrators** or their representatives
[3] **ADM, DADM, CoS,** and the **Executive Assistant Administrators**

Overall, these documents and established processes will increase information sharing across all stakeholders, enhance the transparency of decision-making and security vulnerability mitigation. This will also promote accountability and collaboration as TSA improves consideration of the broad implications of security vulnerabilities and the concerns they pose to our Nation's transportation systems.

Charter Approval

[redacted]

9/11/19
Date

Transportation Security Administration

[redacted]

10 September 2019
Date

Transportation Security Administration

Acting Executive Director
Strategy, Policy Coordination, and Innovation
Transportation Security Administration

[redacted]

09. 10. 19
Date

Director, Enterprise Performance and Risk
Strategy, Policy Coordination, and Innovation
Transportation Security Administration

Transportation
Security
Administration

Risk Management Policy Statement

The Nation's transportation systems are vital to the economic health and security of our country. Protecting the Nation's transportation systems to ensure the freedom of movement for legitimate travelers and commerce is the mission of the Transportation Security Administration (TSA). Implementing effective risk management principles in all modes of transportation and across all functions and programs within TSA is essential to successfully accomplishing this mission.

Our risk-management approach must support our ability to identify, analyze, and appropriately respond to risks across the full spectrum of TSA activities, and leverage the capabilities of our partners to address gaps, reduce vulnerabilities, and mitigate threats. Under the direction of the Chief Risk Officer, working with the Executive Risk Steering Committee, TSA will continue to develop and implement Enterprise Risk Management as the framework for risk management activities across the organization. Through our Enterprise Risk Management program we will:

- Provide a structured, disciplined, and consistent approach to identifying, reporting, assessing, mitigating, and monitoring risk aligned with U.S. Department of Homeland Security guidance.
- Identify, assess, and manage enterprise risks that threaten TSA's achievement of our mission or impede accomplishing our long-term goals and objectives.
- Ensure that enterprise and program risks are managed consistent with defined risk appetite and established risk-tolerance levels.
- Align our strategy, programs, processes, people, technology, information, and budget to maximize the value TSA provides to the Nation.
- Maintain a cross-organizational strategic focus that allows TSA to adapt to changes in risk; rapidly field new operating concepts, performance standards and capabilities; and invest appropriately in our workforce.
- Provide greater transparency into risks by improving our understanding of interactions and relationships between risks, thereby improving risk-based decision making.
- Establish clear accountability and ownership of risk.

Effective risk management is central to the success of TSA's mission and strategic vision, and requires risk management principles be embedded as part of the Agency's culture. To that end, employees are expected to understand and apply the principles of risk management contained in our Enterprise Risk Management program and apply the standards, tools, and techniques consistently across all aspects of TSA. With continued cooperation and commitment to this policy, TSA can best use limited resources to the greatest effect in accomplishing its transportation security mission.

Peter V. Neffenger
Administrator

TSA Risk Appetite Statement

Risk Appetite Statement

The Transportation Security Administration (TSA) risk appetite statement provides broad guidance regarding the amount of risk within a specific area that TSA is willing to accept/pursue in maximizing the value TSA provides to the American people. Risk appetite is considered in different ways depending on whether the risk (uncertainty) being considered represents a threat or an opportunity. When considering threats (unwanted outcomes), risk appetite defines the level of exposure that TSA considers is tolerable. In these instances, TSA will mitigate risk through tight management controls or cautious/conservative policy decisions. Conversely, when considering opportunities (creating or enhancing value), risk appetite defines how much TSA is willing to put at risk in order to realize the desired benefits. In these situations, TSA implements control actions to prevent potential negative impacts from exceeding the level deemed allowable and to monitor if the desired outcomes are being realized. The risk appetite definitions in the following figure help describe the spectrum for the Agency's various levels of risk appetite.

Risk Appetite Definitions

Risk Appetite Approach	Risk Averse	Risk Neutral	Risk Tolerant
Level Of Risk Taking Versus Reward	TSA takes a cautious approach to risk and seeks to avoid negative consequences. TSA sets tight risk tolerance limits, focuses on value preservation, and seeks to minimize risk levels to as low as reasonably practicable.	TSA takes a balanced approach between risk taking and value creation. For risks without great upside or downside potential, TSA sets moderate risk tolerance limits and seeks to avoid over-control.	TSA takes calculated risks to achieve strategic objectives and create additional value. TSA sets wider risk tolerance limits and is willing to accept greater than normal risks to achieve the benefits.
Risk Response Decision Criteria	Minimal calculated risk is accepted. Mitigation actions are taken even though the costs may be greater than the expected consequence, should risk manifest. Employ tight management controls to reduce uncertainty and preserve current value, with cautious and conservative policy decisions.	TSA accepts calculated risks with risk response actions determined based on cost effectiveness, management priorities, and potential outcomes. Management controls are implemented to monitor cost effectiveness and that desired outcomes are being achieved.	Risk response actions are taken to prevent potential losses from exceeding a maximum allowable loss. Controls are implemented to monitor that desired outcomes are being realized.

Transportation Security Administration

Transportation Security Administration Enterprise Risk Management

ERM Policy Manual

March 2016

Contents

Document control information

Document information

Document name	TSA Enterprise Risk Management (ERM) Policy Manual
Document author	TSA Chief Risk Officer
Document version	Version 2
Document status	Final
Date released	

Document edit history

Version	Date	Additions/modifications	Prepared/revised by
1.0	August 2014	Initial Release	OCRO
2.0	January 2016	Update	OCRO

Document review/approval history

Date	Name	Organization/title	Comments

Abbreviations

The following abbreviations are used throughout the document for conciseness:

AA	Assistant Administrator
CMM	Capability Maturity Model
CRO	Chief Risk Officer
DHS	Department of Homeland Security
ERM	Enterprise Risk Management
ERSC	Executive Risk Steering Committee
GPRA	Government Performance and Results Modernization Act
HSE	Health, Safety, and Environment
KPI	Key Performance Indicators
KRI	Key Risk Indicators
OCRO	Office of the Chief Risk Officer
PAR	DHS Performance Accountability Report
TSA	Transportation Security Administration
MRKC	Mission Risk Knowledge Center

Introduction

TSA is implementing Enterprise Risk Management (ERM) to provide a structured, disciplined, and consistent approach to risk management that facilitates risk-informed decision making throughout the organization. ERM provides TSA with a means to align strategy, processes, people, technology, and knowledge for the purpose of evaluating and managing uncertainties in executing our counterterrorism mission. A consistent approach to risk management across the organization is essential for TSA leaders to identify and prioritize strategic risks and for prioritizing competing requirements. ERM enables TSA to more effectively manage enterprise level risks, and it enables agency leaders to consider the trade-offs between risks, associated costs, and value creation across the organization.

This manual explains the TSA approach to establishing a mature and successful ERM program. As TSA's Chief Risk Officer (CRO), I have approved this approach to implementing ERM as the path to achieve mature and sustainable ERM activities and processes. By consistent use of ERM across the organization, TSA will be positioned to identify and assess risks within the current environment through a systematic process which evaluates the impact of risk on TSA's ability to achieve our mission and objectives in support of U.S. Department of Homeland Security (DHS) strategic objectives.

[redacted]

Chief Risk Officer

Purpose of this document

TSA's Enterprise Risk Management Policy Manual (ERM Policy Manual) has two core purposes. First, the ERM Policy Manual defines the foundational elements of TSA's ERM program: TSA's ERM Policy Statement, Risk Appetite Statement, Risk Taxonomy, ERM Framework, and risk management governance structure.

Second, the ERM Policy Manual details the specific roles and responsibilities of TSA leadership, Assistant Administrators, Program Offices, risk management staff, and all TSA employees in implementing ERM throughout the agency. Through the Risk Appetite Statement, the ERM Policy Manual provides guidance to TSA leadership on aligning resource and policy decisions to the amount of risk TSA is willing to accept/pursue within a specific area. Specific details for each of the steps in the ERM framework, along with various risk management tools techniques, and assessment scales are provided in the accompanying ERM Practitioners Guide for use by Program Offices and risk management staff.

The contents of this document provide the evolving blueprint for TSA's ongoing ERM program. Updates to the Policy Manual will be made as the ERM program matures.

ERM Objective

TSA's ERM framework provides the means to embed risk management as a core competency in TSA programs, enabling the agency to fully embed robust and consistent risk management practices at both the enterprise-wide level and within each Program Office in a way that facilitates risk-informed decision making at all levels.

The ERM objectives are to:

- Support TSA leadership through transparency and insight into risks that could impact the ability to execute TSA's mission through the implementation of well-defined and common risk management processes, tools, and techniques.
- Quickly identify both current and emerging risks and develop plans to respond to risks as well as to take advantage of opportunities.
- Increase the likelihood of success in achieving the objectives of TSA's mission and the DHS Strategic Plan.
- Build credibility and sustain confidence in TSA's governance and risk management by all stakeholders including industry, federal, state, and local partners, and the American people.
- Improve the understanding of interactions and relationships between risks.
- Establish clear accountability and ownership of risk.
- Develop the capacity for continuous monitoring and reporting of risk across the Agency from the operational level to the Executive Risk Steering Committee (ERSC).
- Develop a common language and consistent approach across all Program Offices that help to establish the broad scope of risk and to organize risk management activities and reinforces TSA's risk culture.
- Ensure that risks are managed in a manner that maximizes the value TSA provides to the Nation consistent with defined risk appetite and risk tolerance levels.

TSA recognizes that many risks within the organization are interrelated and cannot be effectively and efficiently managed independently within a given Program Office. Instead, these interconnected risks facing TSA must be managed across the organization and, in many instances, in tandem between the agency and its stakeholders. This manual sets forth guidance in the form of repeatable processes and activities to identify, analyze, evaluate, and respond and effectively manage the risks to TSA's mission.

Transportation Security Administration

Enterprise Risk Management Policy Statement

The Nation's transportation systems are vital to the economic health and security of our country. Protecting the nation's transportation systems to ensure the freedom of movement for legitimate travelers and commerce is the mission of the Transportation Security Administration (TSA). Implementing effective risk management principles in all modes of transportation and across all functions and programs within TSA is essential to successfully accomplishing this mission.

Our risk-management approach must support our ability to identify, analyze, and appropriately respond to risks across the full spectrum of TSA activities. Under the direction of the Chief Risk Officer, working with the Executive Risk Steering Committee, TSA will continue to develop and implement Enterprise Risk Management as the framework for risk management activities across the organization. Through our Enterprise Risk Management program we will:

- Provide a structured, disciplined, and consistent approach to identifying, reporting assessing, and monitoring risk aligned with U.S. Department of Homeland Security guidance.
- Identify and manage enterprise risks that threaten TSA's achievement of our mission or impede accomplishing our long-term goals and objectives.
- Ensure that enterprise and program risks are managed consistent with defined risk appetite and established risk-tolerance levels.
- Align our strategy, programs, processes, people, technology, information, and budget to maximize the value TSA provides to the Nation.
- Maintain a cross-organizational strategic focus that allows TSA to adapt to changes in risk; rapidly field new operating concepts performance standards and capabilities; and invest appropriately in our workforce.
- Provide greater transparency into risks by improving our understanding of interactions and relationships between risks thereby improving risk-based decision making.
- Establish clear accountability and ownership of risk.

Effective risk management is central to the success of TSA's mission and strategic vision, and requires risk management principles be embedded as part of the Agency's culture. To that end, employees are expected to understand and apply the principles of risk management contained in our Enterprise Risk Management program and apply the standards, tools, and techniques consistently across all aspects of TSA. With continued cooperation and commitment to this policy, TSA can best use limited resources to the greatest effect in accomplishing its transportation security mission.

Peter V. Neffenger
Administrator

TSA Risk Appetite Statement

The Transportation Security Administration (TSA) risk appetite statement provides broad guidance regarding the amount of risk within a specific area that TSA is willing to accept/pursue in maximizing the value TSA provides to the American people. Risk appetite is considered in different ways depending on whether the risk (uncertainty) being considered represents a threat or an opportunity. When considering threats (unwanted outcomes), risk appetite defines the level of exposure that TSA considers is tolerable. In these instances, TSA will mitigate risk through tight management controls or cautious/conservative policy decisions. Conversely, when considering opportunities (creating or enhancing value), risk appetite defines how much TSA is willing to put at risk in order to realize the desired benefits. In these situations, TSA implements control actions to prevent potential negative impacts from exceeding the level deemed allowable and to monitor if the desired outcomes are being realized. The risk appetite definitions in the following figure help describe the spectrum for the agency's various levels of risk appetite.

Risk Appetite Definitions

Risk Appetite Approach	Risk Averse	Risk Neutral	Risk Tolerant
Level Of Risk Taking Versus Reward	TSA takes a cautious approach to risk and seeks to avoid negative consequences. TSA sets tight risk tolerance limits, focuses on value preservation, and seeks to minimize risk levels to as low as reasonably practicable.	TSA takes a balanced approach between risk taking and value creation. For risks without great upside or downside potential, TSA sets moderate risk tolerance limits and seeks to avoid over-control.	TSA takes calculated risks to achieve strategic objectives and create additional value. TSA sets wider risk tolerance limits and is willing to accept greater than normal risks to achieve the benefits.
Risk Response Decision Criteria	Minimal calculated risk is accepted. Mitigation actions are taken even though the costs may be greater than the expected consequence should risk manifest. Tight management controls to reduce uncertainty and preserve current value, with cautious and conservative policy decisions.	TSA accepts calculated risks with risk response actions determined based on cost effectiveness, management priorities, and potential outcomes. Controls monitor cost effectiveness and if desired outcomes are being achieved.	Risk response actions are taken to prevent potential losses from exceeding a maximum allowable loss. Controls are implemented to monitor that desired outcomes are being realized.

TSA creates value by protecting the Nation's transportation systems while enabling the movement of legitimate travelers and goods. TSA seeks practical and cost-effective solutions to effectively reduce the most significant risks to TSA's ability to achieve its mission.

TSA has different appetites for different risk types expressed in the following statements:

- TSA is averse to security risks that could result in catastrophic consequences.
- TSA is averse to the compromise of classified information.
- TSA is averse to the compromise of Sensitive Security Information (SSI) and Personally Identifiable Information (PII).
- TSA is averse to workforce-related risks pertaining to integrity, performance, health and safety, and regulatory compliance.
- TSA is risk neutral to events that could damage its standing and reputation with the traveling public, US Congress, and other federal, industry, and international stakeholders.
- TSA is risk neutral with regard to other mission and business operational risks.
- TSA is risk tolerant with respect to programs that enhance the movement of legitimate travelers and goods, including supporting acquisitions, technologies, policies, and operational procedures.
- TSA is risk tolerant to efforts that deny exploitation of the Nation's transportation systems for nefarious purposes.

TSA makes risk-informed decisions to achieve its mission within the parameters of its risk appetite:

- TSA evaluates and manages risks to the transportation modes for which it is responsible arising from international or domestic terrorists, insiders, or other adversaries.
- TSA considers the interconnected and interdependent nature of the physical, human, and cyber components of the transportation infrastructure when assessing risks and response plans.
- TSA recognizes that in order to maximize the value provided to the Nation, a systems approach to risk management is necessary to balance security effectiveness with operational efficiency, costs, industry vitality, and resource availability.
- TSA evaluates the highest risk scenarios and the effectiveness of security countermeasures as a system using advanced analytical techniques to apply finite resources commensurate with the risk level and to address gaps and weaknesses in current capabilities.
- TSA strikes a balance between countering known risks and hedging against unknown risks by using strategies such as deploying random and unpredictable security countermeasures, enhancing system resiliency, intelligence-driven targeting rules, and effective vetting programs based on sound identity validation and verification processes.

- TSA maintains a flexible capability to focus resources on the basis of real-time threat information.
- TSA takes decisive action to respond to imminent threats with potentially catastrophic consequences and security effectiveness may take precedence over other considerations.
- TSA evaluates risk levels and implements risk responses and monitoring activities to bring the risk within tolerance without over-controlling non-security related enterprise risks.
- TSA embraces innovation to address adaptive adversaries and changing threats. TSA understands that innovation requires experimentation and balances the need for timely deployment with appropriate testing.

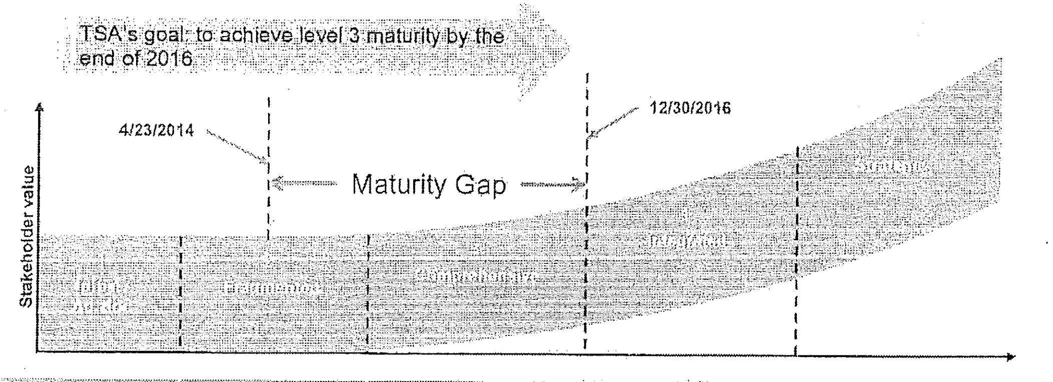
Peter V. Neffenger
Administrator

ERM Maturity

TSA began implementation of ERM in 2014 and is currently concentrating on various targeted initiatives to mature and embed robust and consistent risk management practices within the Program Offices in a way that facilitates risk-informed decision making throughout the organization.

Consistent standards and well-defined roles and responsibilities are central to a successful ERM program. A first step in creating an ERM program is to understand TSA's current risk management practices across the organization and to determine how TSA aligns to our Capability Maturity Model (CMM), designed on industry best practices and tailored to TSA's unique environment. This model contains detailed activities, milestones, attributes and capabilities essential to effective risk management and reflective of levels of maturity: governance, process, people, and technology. Each successive maturity level builds upon the prior level(s) and reflects the evolutionary of ERM from disparate and disconnected efforts, through a comprehensiveness approach to risk management, and leading to a fully integrated risk management program supporting strategic decision-making. These maturity levels define an ordinal scale for evaluating and measuring the maturity of an enterprise's capabilities, and also help to prioritize improvement efforts. The increasing levels of sophistication generally require that leadership dedicate increased time, resources, and executive commitment to implement.

Figure 1: TSA ERM Maturity Model



Initial/Ad hoc	Fragmented	Comprehensive	Integrated	Strategic
• Risk management activities are ad hoc • No overarching risk management philosophy or objectives are defined	• Risk management functions independently within business units • Risk types managed are limited to hazard, financial, and compliance	• Risk management is enterprise-wide and encompasses all risk types including strategic and operational • Common standards, tools an techniques implemented • Risk appetite and risk tolerance set for all risk types and strategic risks	• Risks are treated as a portfolio at the enterprise level and are correlated and aggregated across risk types and business units	• Incorporated into capital allocation, product development. etc. • Early warning risk indicators • Linkage to performance measurement/incentives • Risk modeling/scenarios • Technology implementation • Industry benchmarking

Using the approved CMM, an assessment of TSA's maturity level was completed in mid-2014, and determined that overall, our risk management practices across the agency were at the Level 2 (Fragmented) maturity level. This level is consistent with an enterprise that is in the process of initiating an ERM program. TSA has established the goal of reaching Level 3 (Comprehensive) by the end of calendar year 2016, with a longer-range goal of achieving maturity Level 4 (Integrated) by the end of calendar year 2021. A follow-on maturity assessment in mid-2015 showed the agency was making steady progress towards achieving our 2016 goal.

TSA continues to focus on specific areas to advance its maturity towards the Comprehensive level by the end of calendar year 2016. During 2014 and 2015, efforts centered on establishing the ERM infrastructure and capabilities. Specifically, TSA:

- Approved ERM policy and defined the ERM organizational structure and policy manual,
- Established risk appetite statements and developed risk tolerance thresholds in line with risk appetite,
- Defined enterprise risk assessment criteria,
- Developed risk reporting process and templates,
- Amended performance measures to embed risk management responsibilities and goals,
- Defined high-level requirements for ERM information system.

Building on this ERM foundation, TSA then focused on implementing the ERM process across the Agency through various initiatives as:

- Performing enterprise risk identification through multi-disciplinary stakeholder working groups,
- Assessing enterprise risks using quantitative and qualitative methods,
- Prioritizing risks, assign risk owners, and develop response plans aligned to TSA risk tolerance thresholds,
- Finalizing requirements and perform ERM IT support system selection ,
- Developing Key Risk Indicators (KRIs),
- Developing and disseminating a risk culture survey with action plans based on results,
- Developing and implementing risk management training for all TSA employees.

During 2016, TSA will concentrate on operating, sustaining, and maturing ERM capabilities by:

- Implementing risk response plans and tracking progress against risk objectives for Programs,
- Performing dynamic monitoring of KRIs to assess potential for risk events in line with established risk tolerance thresholds,
- Performing on-going risk reporting to inform decision making at the enterprise level
- Building further linkages between ERM, internal controls, and resource allocation processes to embed risk-based decision-making throughout the organization,
- Determining hardware, software, and environment requirements for ERM IT support system and preparing for installation,

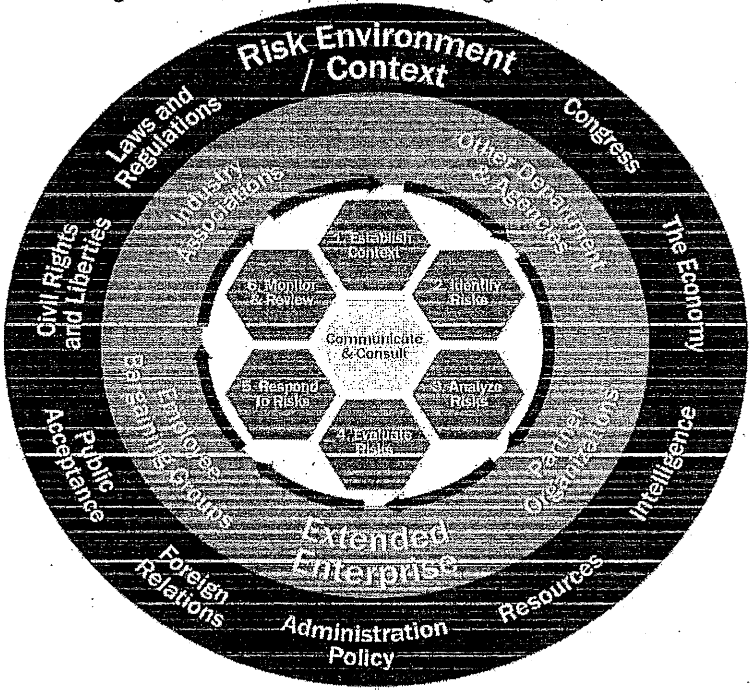
- Continuing to build organizational capacity through external training, disseminating leading research and practices, and professional networking and knowledge-sharing (TSA Risk Community of Interest),
- Implementing ERM training for appropriate staff and collaborating with other TSA offices to embed targeted risk management techniques and decision-making tools into existing training, and
- Developing implementation plans to achieve maturity level 4 by the end of 2021.

ERM Process Framework

Managing risk is not linear and does not take place in a vacuum. Rather, effective risk management represents the balancing of a number of interwoven internal and external factors which shape the risk environment and decision context, and limit risk response alternatives. Furthermore, specific risks cannot be addressed in isolation from each other; the management of one risk may have an impact on another, or management actions which are effective in controlling more than one risk simultaneously may be achievable.

The ERM process framework depicted below is being implemented by TSA. It is closely aligned with the DHS Risk Management Process[1] and incorporates elements from the International Standards Organization (ISO) 31000:2009 Risk Management — Principles and Guidelines and the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management Integrated Framework (2004). By necessity, the model represents the risk management process as discrete sub-elements for illustrative purposes, but in reality they blend together. In addition, the particular stage in the process which one may be at for any particular risk will not necessarily be the same for all risks.

Figure 2: TSA Enterprise Risk Management Process



[1] Beers, R.,(2011), *Risk Management Fundamentals, Homeland Security Risk Management Doctrine*, U.S. Department of Homeland Security, Washington, D.C., April 2011, p. 15

This model also illustrates how the core risk management process is not isolated, but takes place in a context; and, how certain key elements have to be given careful consideration in order for the overall process to generate the outcomes desired from risk management. Risk management must function in an environment in which risk appetite has been defined. The concept of risk appetite (how much risk is tolerable and justifiable) should be regarded as an "overlay" across the whole of this model.

This risk management process provides a logical and systematic method for establishing the context for risks, as well as identifying, analyzing, evaluating, responding to, monitoring, and communicating them in a way that will allow TSA to make decisions and respond timely to risks and opportunities as they arise. This approach promotes comparability and a shared understanding of information and analysis in the decision process and facilitates a better risk management structure and risk-informed decision making. A high level description of each process step within the ERM framework is presented below.

Establish the Context

The *Establish the Context* process step involves understanding and articulating the internal and external environment of the organization. During this step, TSA defines its objectives, evaluates the external and internal parameters to be taken into account when managing risk, makes changes to the risk management process, and develops risk criteria.

Identify Risks

During the *Identify Risks* process step, TSA seeks to identify enterprise-level risks to be managed using a structured, systematic process called the Enterprise Risk Register. This process specifies what risks can occur, as well as where, when, why, and how they may occur. The list of risks identified through this process is preliminary and subject to further qualification and refinement as part of the following *Analyze Risks* process. The *Identify Risks* process captures risks using TSA's enterprise risk taxonomy and then progressively narrows the list to the most critical using first qualitative and then quantitative techniques in the *Analyze Risks* process.

Analyze Risks

The *Analyze Risks* process involves consideration of the causes and sources of risk, the probability that the risk event will occur, their positive or negative consequences and magnitude, and the likelihood that those consequences may occur. Risk analysis provides the basis for evaluation and decisions regarding risk response or treatment. Each risk identified during the *Identify Risks* process is subjected to a qualitative evaluation of its likelihood and impacts. The list of risks is then narrowed and refined based on the criticality of the risk. Those risks falling below a defined threshold may continue to be monitored and managed within TSA, but will not be reported at the executive level as part of the Enterprise Risk Register.

Evaluate Risks

The *Evaluate Risks* process uses the qualitative risk analysis generated in the preceding *Analyze Risk* process to rank and prioritize enterprise level risks. By prioritizing the enterprise-level risks, TSA leadership can respond as appropriate with strategic allocation of resources in the *Respond to Risks* process. Usually, risk managers find that responding to a few critical risks results in dramatic reductions in residual risk. During *Evaluate Risks*, TSA leadership should revisit the documented risk tolerances in light of their overall risk portfolio and make adjustments.

Respond to Risks

The *Respond to Risks* process involves identifying and assessing the range of risk response options and preparing implementation plans for selected response options. Responding to risks includes both the seizing of opportunities to achieve mission success as well as efforts to minimize the adverse impacts of risk. Using a prioritized list of quantified risks requiring response options from the *Evaluate Risks* process, TSA leadership can make informed strategic decisions about how to allocate resources to programs and projects reflected in the enterprise risk register.

Monitor and Review

The *Monitor and Review* process involves ongoing review risk management efforts and response strategies to ensure they remain relevant and effective. Factors that may affect the likelihood and consequences of an outcome may change over time, as may the factors that affect the suitability or cost of the selected response options. It is therefore necessary to repeat the risk management cycle regularly. *Monitor and Review* also involves benchmarking actual ERM risk management outcomes against expected or required performance levels.

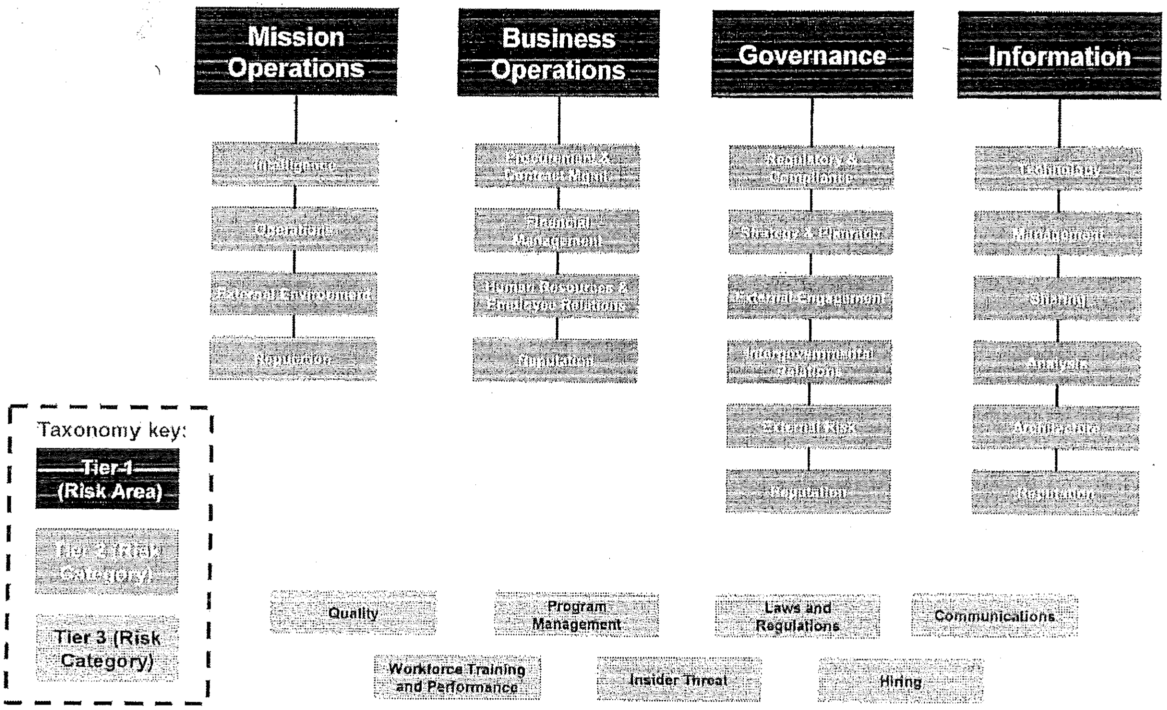
Communicate and Consult

Communication and Consultation are intrinsic to the risk management process and should be considered at each step. Clear communication channels are essential to fully integrating risk management in all Program Offices and to developing a culture where the positive and negative dimensions of risk are recognized and valued.

ERM Risk Taxonomy

The ERM Risk taxonomy organizes risk into categories to promote consistent identification, assessment, measurement, and monitoring of risks across the organization. Using a common and consistent risk taxonomy across the entire organization enables TSA to determine the relationships between various risks in a manner that allows improved assessment of the overall impact to the organization. Figure 3 illustrates TSA's ERM risk taxonomy, including 3 tiers of risk categories. The four tables that follow further define the Tier 2 risk categories within each Tier 1 risk area. Taxonomy tiers are intended to provide increasing levels of detail for a specific risk, and do not denote levels of importance.

Figure 3: Risk Taxonomy



ERM Roles and Responsibilities

TSA Administrator

The TSA Administrator maintains ultimate accountability for the management of the agency's risks, including issuing directives for their management. The Administrator also authorizes and owns the TSA ERM Policy and issues final approval of the ERM risk appetite statements.

Executive Risk Steering Committee (ERSC)

The role of the ERSC, chaired by the CRO and composed of all Assistant Administrators (AAs) is to oversee the development and implementation of processes used to analyze, prioritize, and address risks across TSA. These risks include terrorism threats facing the entire transportation sector, along with non-operational risks that could impede TSA's ability to achieve its strategic objectives. The ERSC is broadly responsible for ensuring that risks are managed to create value for the Nation and in a manner consistent with established risk appetite and risk tolerances levels. Specific duties and responsibilities are depicted in the ERSC Charter attached as Appendix 1 to this manual.

Chief Risk Officer (CRO)

The CRO serves as the principal advisor to the Administrator and Deputy Administrator on all risk matters that could impact TSA's ability to perform its mission. The CRO is responsible for the design, development, and implementation of the ERM program at TSA and ensuring TSA is in compliance with federal risk management guidance, such as OMB Circular A-123. The CRO, in conjunction with the TSA ERM Team, will lead TSA in conducting regular enterprise risk assessments of TSA business processes or programs at least quarterly and will oversee the identification, assessment, prioritization, response, and monitoring of enterprise risks, which includes the development of enterprise level Key Risk Indicators (KRIs). In addition, the CRO will oversee the implementation and monitoring of the TSA-wide Centralized Security Vulnerability Management process. The CRO will also lead TSA strategic planning and integration of risk-based security (RBS) and risk management (RM) principles across the enterprise. The CRO will collaborate with the Chief Financial Officer to align ERM and resource allocation decision-making processes. The CRO will review the TSA Risk Register, ERM Policy Statement, and Risk Appetite Statement every year at a minimum and provide recommended changes for consideration and comment by the ERSC prior to finalizing any future revisions.

Assistant Administrators (AAs)

AAs, who comprise TSA's Senior Leadership Team (SLT), serve as ultimate risk owners in accordance with the ERSC Charter. Program Offices will adopt and follow the ERM framework and the TSA ERM Policy and participate in enterprise-wide risk management efforts and perform risk management activities within their individual office. AAs are responsible for implementing consistent risk management practices in alignment with this policy, including but not limited to the following:

- Establishing and updating at least annually a Program Office-level risk register and submitting the risk register to OCRO for review;
- Escalating risks to OCRO for consideration as additions to the TSA Risk Register;
- Implementing Program Office-level processes to identify systemic security vulnerabilities, in support of the Centralized Security Vulnerability Management process;
- Integrating considerations of risk into Program Office resource allocation decision-making and strategic planning processes; and
- Aligning management control techniques to Program Office risks and ensuring these techniques are integrated into the Management Control Objective Plan program.

It is also the responsibility of the Program Offices to disaggregate the enterprise level risk appetite statements into Program Office specific risk limits, where applicable, and develop and monitor Key Performance Indicators (KPIs) and KRIs. Program Offices and AAs will also assist the ERM Team by nominating Subject Matter Experts (SMEs) to serve on risk assessment teams during the risk identification, analysis, and evaluation processes. AAs will serve as Risk Owners for assigned enterprise level risks and will be responsible for the implementation and monitoring of risk response strategies and associated KRIs.

OCRO/ ERM Branch

The ERM Branch (ERM Team) resides within OCRO and leads ERM activities under the supervision of the CRO. Such activities include developing and maintaining ERM policies, processes, procedures, tools, and information systems; leading efforts to perform enterprise risk identification, assessment, prioritization, reporting, and monitoring; establishing enterprise level KRIs; and, establishing ERM communication at all levels and for gathering data and developing risk reports. The ERM Branch is also responsible for managing the agency-wide implementation of the Centralized Security Vulnerability Management process.

Program Office ERM Liaisons

Program Office ERM Liaisons are designated individuals within each TSA Program Office that serve as the primary representative to the ERM Team. ERM Liaisons are responsible for communicating with the ERM Team and supporting Program Office risk owners throughout the ERM process, as necessary. They also serve as an advisory body that shares information and provides subject matter expertise to support ERM program activities, such as the identification, validation, and assessment of enterprise risks.

Risk Analysis Integrated Project Team (IPT)

Risk Analysis IPTs are comprised of cross-functional subject matter experts (SMEs) that are responsible for assessing a defined enterprise risk to identify cross-functional root causes and consequences. IPT members will assist the ERM Team and Risk Owners to develop event trees or scenarios, estimate probabilities and impacts, identify risk response options, perform cost-benefit analysis, identify Key Risk Indicators (KRIs), and develop recommendations for risk response and monitoring plans for enterprise risks.

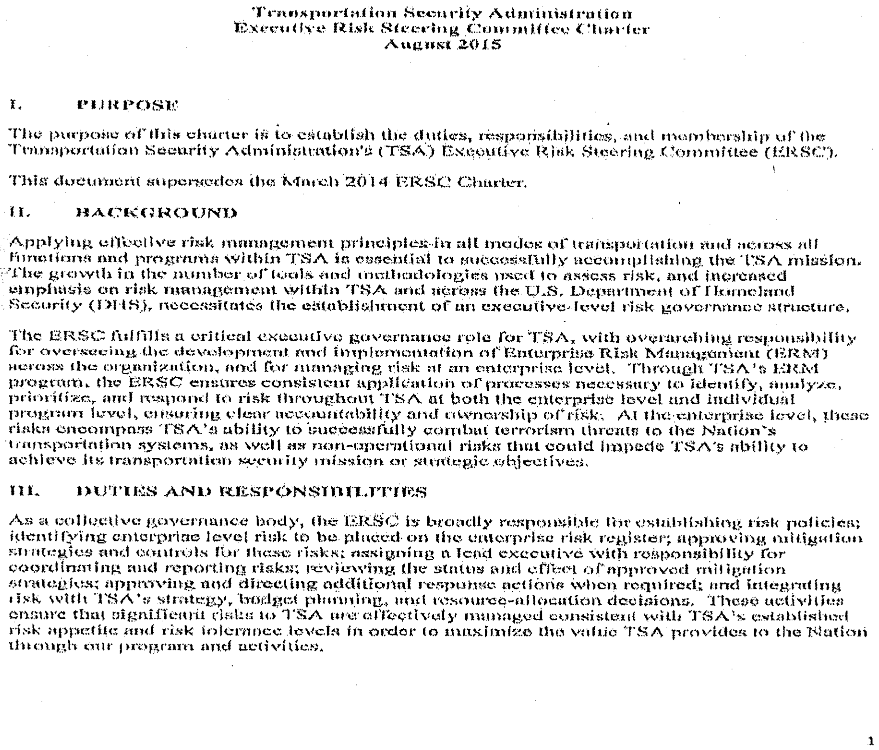
TSA Employees

Effective ERM programs require both leadership and employees to actively own and commit to the success of the program. As such, it is the responsibility of all TSA employees to complete required risk management training which is designed to enable every TSA employee to integrate risk-based decision-making principles into their daily work.

Related Laws, Regulations, and Policy Exceptions

ERM policies, procedures, and activities must comply with Government Statutes and Laws as well as requirements dictated by the U.S. Congress, U.S. Department of Homeland Security (DHS), U.S. Government Accountability Office (GAO), and other relevant stakeholders. Any exception to this policy must be documented in writing and approved by the AA of the Program Office and forwarded to the CRO for notification, review, and approval. The Risk Management Division of the OCRO will track policy exceptions and report this status to the ERSC. Additionally, policy exceptions must be reviewed and approved by TSA's SLT.

Appendix 1: ERSC Charter



Transportation Security Administration
Executive Risk Steering Committee Charter
August 2015

I. PURPOSE

The purpose of this charter is to establish the duties, responsibilities, and membership of the Transportation Security Administration's (TSA) Executive Risk Steering Committee (ERSC).

This document supersedes the March 2014 ERSC Charter.

II. BACKGROUND

Applying effective risk management principles in all modes of transportation and across all functions and programs within TSA is essential to successfully accomplishing the TSA mission. The growth in the number of tools and methodologies used to assess risk, and increased emphasis on risk management within TSA and across the U.S. Department of Homeland Security (DHS), necessitates the establishment of an executive-level risk governance structure.

The ERSC fulfills a critical executive governance role for TSA, with overarching responsibility for overseeing the development and implementation of Enterprise Risk Management (ERM) across the organization, and for managing risk at an enterprise level. Through TSA's ERM program, the ERSC ensures consistent application of processes necessary to identify, analyze, prioritize, and respond to risk throughout TSA at both the enterprise level and individual program level, ensuring clear accountability and ownership of risk. At the enterprise level, these risks encompass TSA's ability to successfully combat terrorism threats to the Nation's transportation systems, as well as non-operational risks that could impede TSA's ability to achieve its transportation security mission or strategic objectives.

III. DUTIES AND RESPONSIBILITIES

As a collective governance body, the ERSC is broadly responsible for establishing risk policies; identifying enterprise level risk to be placed on the enterprise risk register; approving mitigation strategies and controls for these risks; assigning a lead executive with responsibility for coordinating and reporting risks; reviewing the status and effect of approved mitigation strategies; approving and directing additional response actions when required; and integrating risk with TSA's strategy, budget planning, and resource-allocation decisions. These activities ensure that significant risks to TSA are effectively managed consistent with TSA's established risk appetite and risk tolerance levels in order to maximize the value TSA provides to the Nation through our program and activities.

The primary functions of the ERSC are to assist the Administrator and Deputy Administrator in oversight of Key Agency risks through the following responsibilities:

- Developing, implementing, and applying TSA's ERM Policy;
- Ensuring the effective operation of the ERM Framework and setting the tone for risk management throughout TSA;
- Recommending the risk appetite and associated risk-tolerance level for each major category of risk associated with TSA's strategic objectives;
- Setting the risk-based security and risk-management strategies for TSA and providing strategic oversight;
- Identifying, prioritizing, and monitoring the most significant enterprise risks reflected through the strategic risk register and ensuring appropriate risk response and mitigation plans are working to achieve desired outcomes;
- Identifying, mitigating, and monitoring the top strategic enterprise risks reflected on the Agency's Enterprise Risk Register;
- Sponsoring and providing oversight, direction, and review for working groups and assessment teams tasked with analyzing specific risks and/or related policies; and,
- Aligning risk with TSA's strategy, budget planning, and resource allocation decisions.

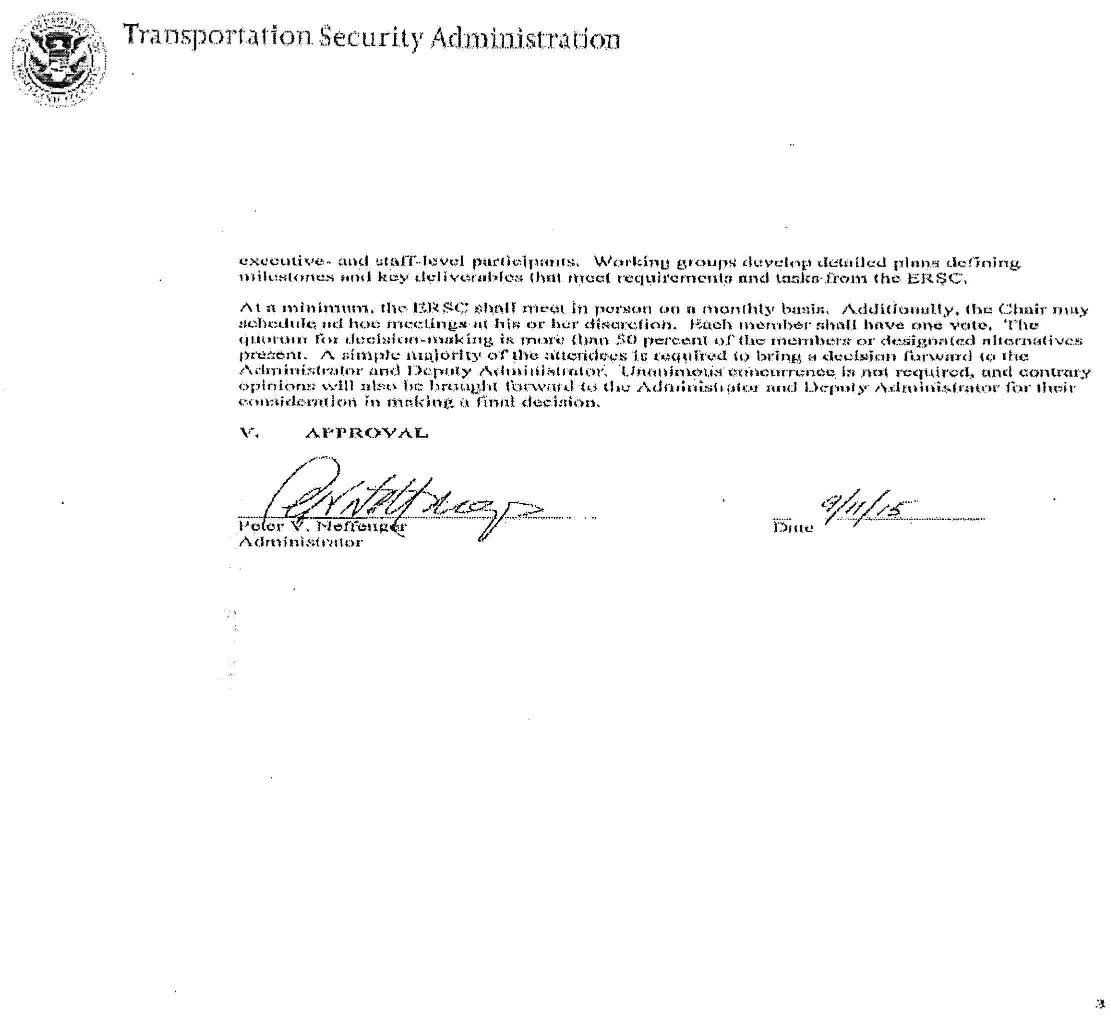
As TSA executives, ERSC members are responsible for managing risks within their respective program offices. However, when participating as a member of the ERSC, they have an obligation to consider risk management from an Agency-wide perspective. Specified duties of ERSC members include:

- Attending ERSC meetings in person or appointing a designated alternate empowered to make decisions. Prior approval from the Chair is needed should this person be below the level of Deputy Assistant Administrator.
- Appointing knowledgeable and empowered representatives and a designated alternate to participate on working groups and assessment teams established by the ERSC.
- Elevating major risk-related decisions to the full ERSC as necessary.
- Reviewing read-ahead materials prior to the meeting.
- Facilitating ERM-related communications within their respective program offices.

IV. ORGANIZATION

ERSC membership includes all Assistant Administrators as the scope of TSA's risk management efforts is enterprise-wide. Deputy Assistant Administrators may attend ERSC meeting as a non-voting participant and will serve as the alternate to their Assistant Administrator. Other subject-matter experts and briefers will participate in specific meetings as deemed necessary when requested by an ERSC member and approved by the Chief Risk Officer.

The Chief Risk Officer will serve as the Chair for all ERSC meetings. When the Chief Risk Officer is unavailable, an Assistant Administrator will be designated to lead the ERSC meeting. A project management staff supports the Chair in preparing for and conducting the ERSC meetings. As required, the ERSC oversees the progress of working groups that consist of



Transportation Security Administration

executive- and staff-level participants. Working groups develop detailed plans defining milestones and key deliverables that meet requirements and tasks from the ERSC.

At a minimum, the ERSC shall meet in person on a monthly basis. Additionally, the Chair may schedule ad hoc meetings at his or her discretion. Each member shall have one vote. The quorum for decision-making is more than 50 percent of the members or designated alternatives present. A simple majority of the attendees is required to bring a decision forward to the Administrator and Deputy Administrator. Unanimous concurrence is not required, and contrary opinions will also be brought forward to the Administrator and Deputy Administrator for their consideration in making a final decision.

V. APPROVAL

Peter V. Neffenger
Administrator

Date 9/11/15

Office of Chief Risk Officer
Enterprise Risk Management
How It Works

Enterprise Risk Management (ERM) Program POCs

[redacted]

ERM Branch Manager

[redacted]

[redacted]

ERM Team Lead

[redacted]

[redacted]

Strategy and Governance Team Lead

[redacted]

[redacted]

ERM Support

[redacted]

[redacted]

ERM Support

[redacted]

[redacted]

ERM Support

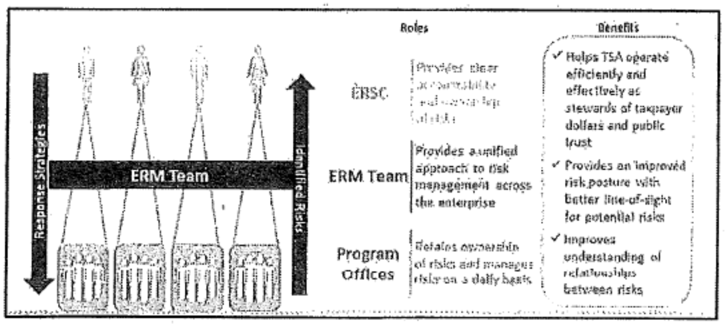
[redacted]

Office Email

[redacted]

Enterprise Risk Management at TSA – How It Works

The TSA Administrator and Deputy Administrator maintain ultimate accountability for the agency's risk management. The Administrator owns the TSA ERM policy and issues final approval of ERM risk appetite statements. The Chief Risk Officer manages the ERM program at the enterprise level.



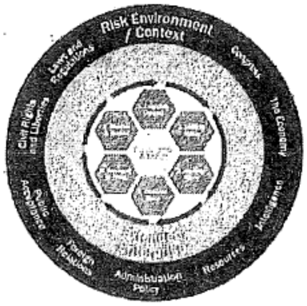
	Roles	Benefits
ERSC	Provides clear accountability and ownership of risks	✓ Helps TSA operate efficiently and effectively as stewards of taxpayer dollars and public trust
ERM Team	Provides a unified approach to risk management across the enterprise	✓ Provides an improved risk posture with better line-of-sight for potential risks
Program Offices	Retains ownership of risks and manages risks on a daily basis	✓ Improves understanding of relationships between risks

Key Players

- Executive Risk Steering Committee (ERSC) – The governing body for ERM at TSA.
- Chief Risk Officer (CRO) – Oversees the Office of Chief Risk Officer (OCRO) ERM Team and manages TSA's ERM program.
- OCRO-ERM Team – Responsible for implementing TSA's ERM program.
- Program Office Liaisons – TSA Program Office representatives that serve as liaisons to OCRO.
- Risk Analysis Integrated Project Teams (IPTs) – Cross-functional Subject Matter Experts (SMEs) responsible for identifying and analyzing enterprise risks.
- Risk Owners – Provide subject matter expertise for assigned enterprise risks.

TSA's Enterprise Risk Management Process

TSA's risk management process provides a logical and systematic method for establishing the context for risks, as well as identifying, analyzing, evaluating, responding to, monitoring, and communicating them in a way that allows TSA to make decisions and sensibly respond to opportunities and risks as they arise.



Enterprise Performance & Risk

Enterprise Risk Management Overview

Enterprise Risk Management Program POCs

[redacted]

Director
Enterprise Performance & Risk

[redacted]

[redacted]

Analyst
Enterprise Performance & Risk

[redacted]

[redacted]

Analyst
Enterprise Performance & Risk

[redacted]

Office Email

[redacted]

Enterprise Risk Management

Enterprise Risk Management (ERM) is a comprehensive approach to risk management that engages organizational systems and processes together to improve the quality of decision making for managing risks.

Within TSA and between TSA and external organizations risk is often cross-functional. Typical risk events, while inherent to one function or program office, can affect multiple areas of our organization or the transportation domain. TSA's ERM policy explains risk management is an essential element to achieving TSA's mission and is an effective, simple, and practical framework for managing risks that impact our agency's ability to achieve its mission.

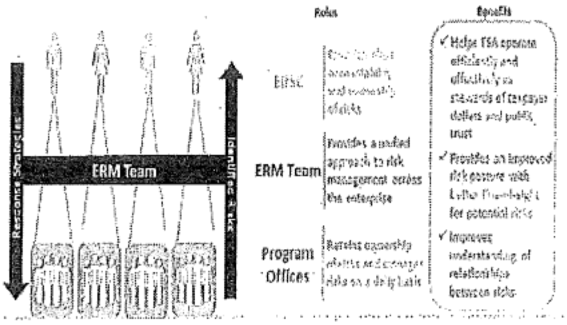
ERM Objectives

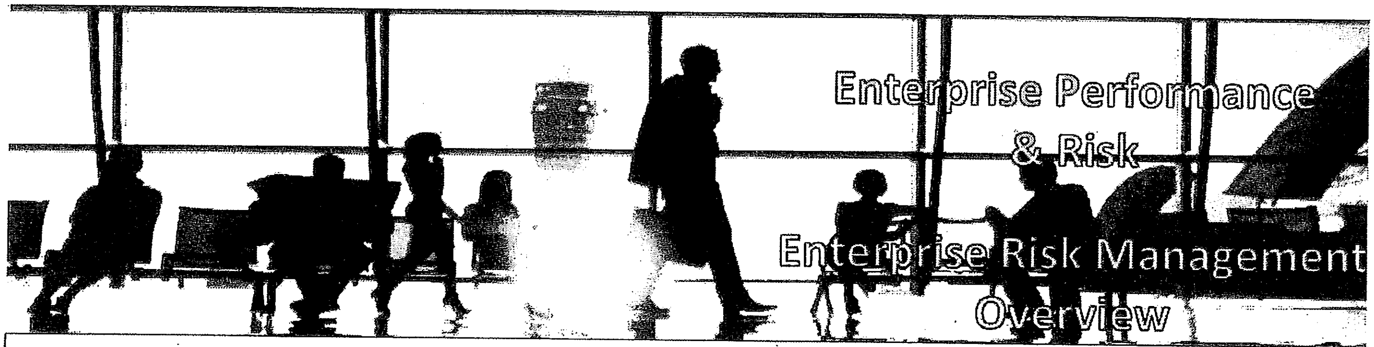
ERM provides a structured, disciplined, and consistent approach to assess risk aligned with DHS guidance. ERM objectives include:

- Identifying and managing strategic risks that threaten TSA's achievement of long-term objectives and goals.
- Ensuring risks are managed in a manner that maximizes the value TSA provides to the nation.
- Aligning strategy, process, people, technology, and information.
- Providing greater transparency into risks by improving understanding of interactions and relationships between risks and risk-based decision making.
- Establishing clear accountability and ownership of risk.

ERM at TSA – How It Works

The TSA Administrator and Deputy Administrator maintain ultimate accountability for the agency's risk management. The Administrator owns the TSA ERM policy and issues final approval of ERM risk appetite statements. The Chief Risk Officer manages the ERM program at the enterprise level.

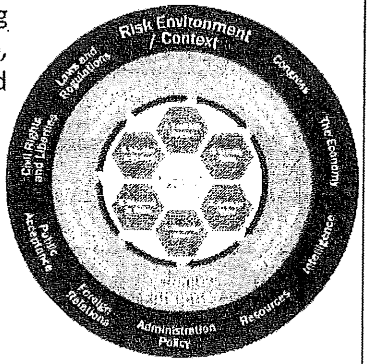

Roles
Benefits
Response Strategies
ERM Team
Identifies Risks
EPRC
Provides clear accountability and ownership of risks
ERM Team
Provides a unified approach to risk management across the enterprise
Program Offices
Retains ownership of risks and manages risks on a daily basis
✓ Helps TSA operate efficiently and effectively as stewards of taxpayer dollars and public trust
✓ Provides an improved risk posture with better foresight for potential risks
✓ Improves understanding of relationships between risks



Enterprise Performance & Risk

Enterprise Risk Management Overview

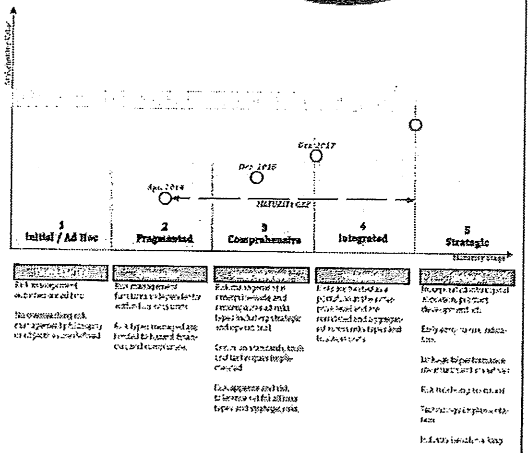
TSA's ERM Process



TSA's risk management process provides a logical and systematic method for establishing the context for risks, as well as identifying, analyzing, evaluating, responding to, monitoring, and communicating them in a way that allows TSA to make decisions and sensibly respond to opportunities and risks as they arise.

Key players in the risk process include the:

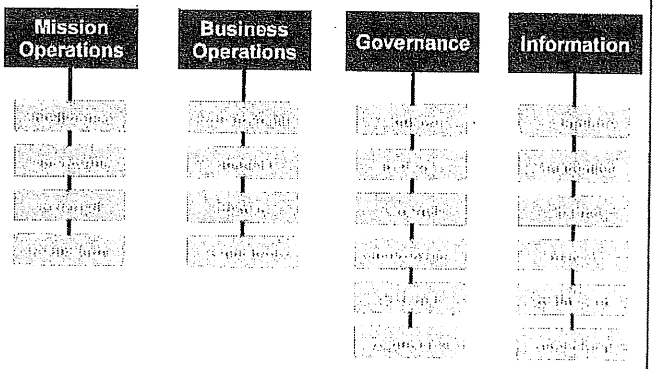
- Executive Risk Steering Committee (ERSC) – The governing body for ERM at TSA.
- Executive Director of Strategy, Policy Coordination, & Innovation (SP&I) – Oversees the Enterprise Performance & Risk (EPR) ERM Team and manages TSA's ERM program.
- EPR-ERM Team – Responsible for implementing TSA's ERM program.
- Program Office Liaisons – TSA Program Office representatives that serve as liaisons to EPR.
- Risk Assessment Integrated Project Teams (IPTs) – Cross-functional Subject Matter Experts (SMEs) responsible for identifying and analyzing enterprise risks.
- Risk Owners – Provide subject matter expertise for assigned enterprise risks.



ERM Maturity Model

TSA's ERM maturity model is divided into 5 levels. This diagram communicates the high-level characteristics of each level.

TSA achieved level 4, "comprehensive" maturity at the end of 2017 and EPR intends to reach level 5, "strategic" maturity by 2021. Leveraging the professional expertise of the ERM Team, Program Office Liaisons, and Cross-functional IPTs provides TSA the best opportunity for realizing this goal.



ERM Taxonomy

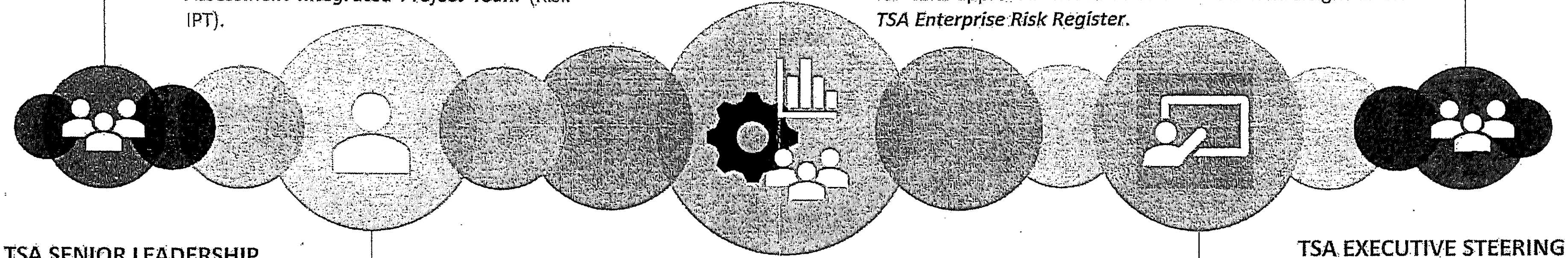
The diagram to the right is a visualization of the ERM Risk Taxonomy. The ERM taxonomy includes three standard tiers

- Tier 1 Risk Area – Main risk areas
- Tier 2 Risk Category – Risk categories

The ERM Risk Taxonomy is based on the ERM Policy Manual, the Risk Management Training Manual and industry standards.

Updated December 2018

TSA Enterprise Risk Management



01

TSA SENIOR LEADERSHIP

All TSA enterprise risk assessment requests typically originate from TSA Senior Leadership. Requests may come from the *TSA Front Office*, the ***TSA Executive Steering Committee (ESC)****, or* the ***Executive Risk Steering Committee (ERSC)***. The ***Chief Risk Officer*** (CRO) or any individual program office's AA or EAA may also originate a risk assessment request.

02

TSA CHIEF RISK OFFICER

The ***TSA Chief Risk Officer*** (CRO) is the senior risk expert in the Agency and serves as the Chair of the ***TSA Executive Risk Steering Committee*** (ERSC). The CRO provides also oversight of the ***TSA Risk Assessment Integrated Project Team*** (Risk IPT).

03

TSA RISK ASSESSMENT INTEGRATED PROJECT TEAM

The ***TSA Risk Assessment Integrated project Team*** (Risk IPT) analyses the enterprise risk assessment request during its bi-weekly meetings. The Risk IPT is made up of SME representation from every TSA program office. Each risk assessment may take several (2-5) meetings to complete the research and craft the risk assessment (3-7) questions, focused on ***Threat, Vulnerability***, and ***Consequence***, taking ***Likelihood*** and ***Impact*** into consideration. Quantitative risk scores are elicited from the Risk IPT SMEs via Poll Everywhere®. The Risk IPT also maintains the ***TSA Security Vulnerability Management Process*** (SVMP).

04

TSA EXECUTIVE RISK STEERING COMMITTEE

The ***TSA Executive Risk Steering Committee*** (ERSC) is a monthly meeting with TSA Senior Leadership. Enterprise risk assessment analysis results and mitigation implementation plans are briefed to the ERSC for guidance and concurrence. Once approved, recommendations are forwarded to the ***TSA Executive Steering Committee*** (ESC) for final approval. The ERSC also maintains oversight of the ***TSA Enterprise Risk Register.***

05

TSA EXECUTIVE STEERING COMMITTEE

The ***TSA Executive Steering Committee*** (ESC) is made up of the ***TSA Deputy Administrator, TSA Chief of Staff, Executive Assistant Administrators***, and Advisors. The group provides the final approval of TSA risk assessments and all modifications to the ***TSA Enterprise Risk Register.***

Strategy, Policy Coordination, and Innovation (SP&I)
Enterprise Performance and Risk (EPR)

Filename: TSA Enterprise Risk Management—03.19.19

TSA Security Vulnerability Management Process

02 - Strategy

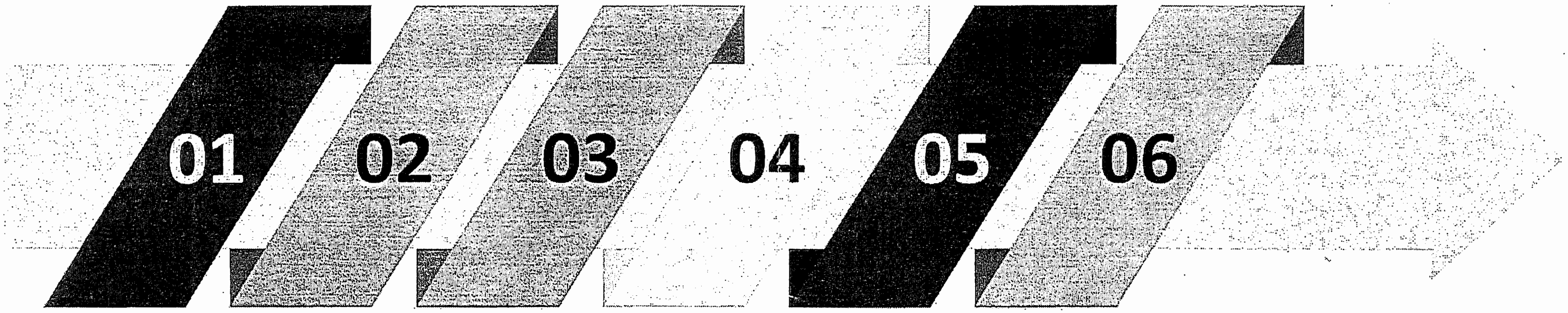
Within **30 days** of submission, the TSA **Mitigation Strategy Team**[1] (MST) meets to determine the context, prioritization, and appropriate security vulnerability mitigation strategy; also recommends a **Vulnerability Owner.**

04 - Execution

The **Vulnerability Owner** takes action to mitigate or resolve the security vulnerability in order to accomplish the milestones and target deadlines established by the **ERSC.**

06 - Resolution

Once resolved and approved by the ESC, **Strategy, Policy Coordination, and Innovation** (SP&I) archives the security vulnerability, incorporates data into the **Planning, Programming, Budgeting and Execution** (PPBE) process, and then removes it from the **SVMP** tracker report.



01 - Identification

Any TSA **Program Office** may submit a security vulnerability for consideration via the standardized TSA intake form.

03 – Governance

Within **60 days** of submission, the TSA **Executive Risk Steering Committee**[2] (ERSC) makes the final determination regarding formal mitigation actions, milestones, resourcing, prioritization, target deadlines, and **Vulnerability Owner.**

05 – Review

The TSA **ERSC** reviews the **Security Vulnerability Management Process** (SVMP) tracker report on a quarterly basis to monitor security vulnerability mitigation progress and provides updates to the TSA **Executive Steering Committee**[3] (ESC).

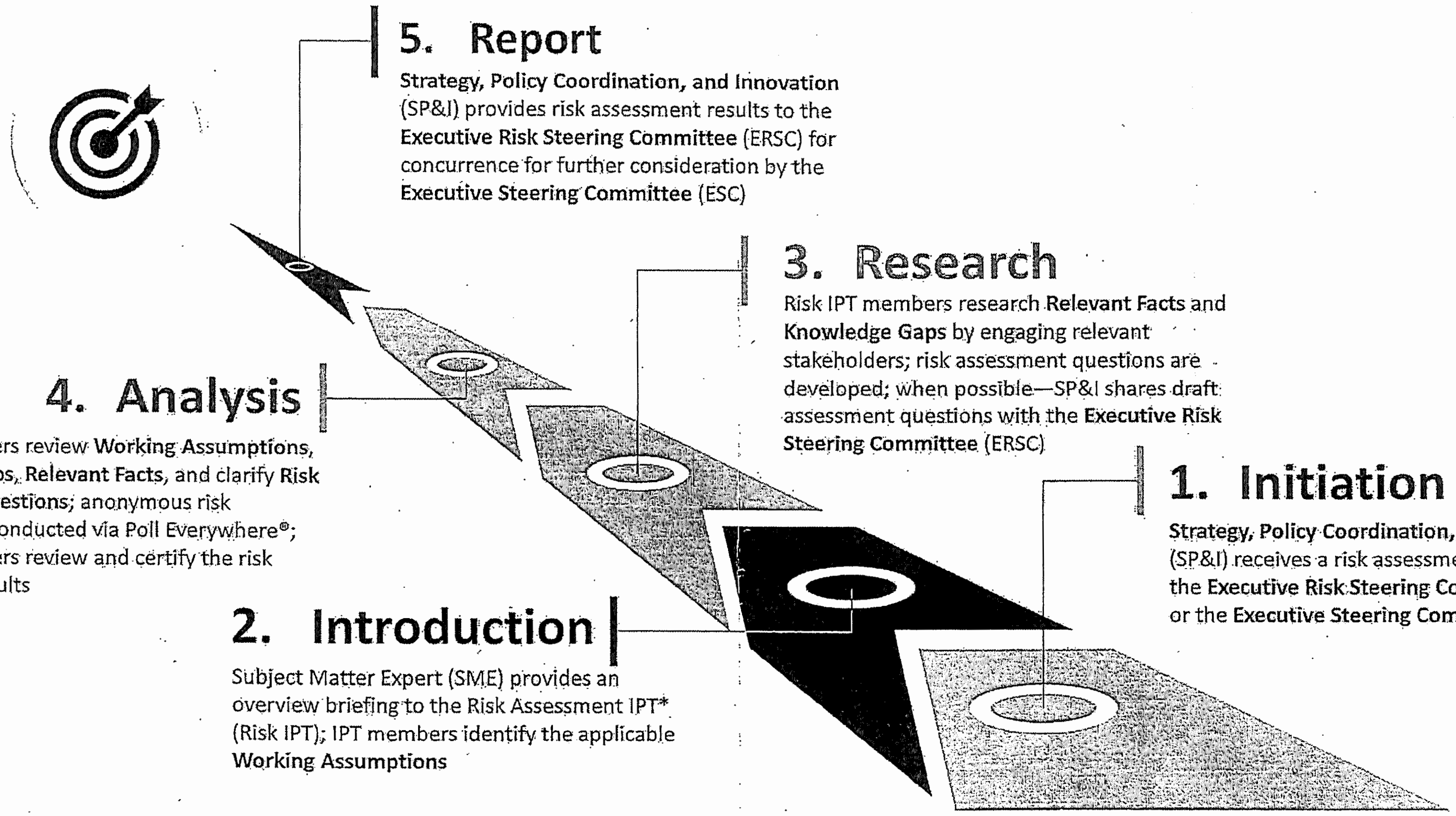
DRAFT

Strategy, Policy Coordination, and Innovation (SP&I)
Enterprise Performance and Risk (EPR)

Filename: SVMP Resolution Process - 03.14.19

[1] SP&I, RCA, INS, and the Vulnerability Owner
[2] Assistant Administrators or their Representatives
[3] DADM, CoS, and the Executive Assistant Administrators

TSA Risk Assessment IPT Process



1. Initiation

Strategy, Policy Coordination, and Innovation (SP&I) receives a risk assessment request from the **Executive Risk Steering Committee** (ERSC) or the **Executive Steering Committee** (ESC)

2. Introduction

Subject Matter Expert (SME) provides an overview briefing to the Risk Assessment IPT* (Risk IPT); IPT members identify the applicable **Working Assumptions**

3. Research

Risk IPT members research **Relevant Facts** and **Knowledge Gaps** by engaging relevant stakeholders; risk assessment questions are developed; when possible—SP&I shares draft assessment questions with the **Executive Risk Steering Committee** (ERSC)

4. Analysis

Risk IPT members review **Working Assumptions**, **Knowledge Gaps**, **Relevant Facts**, and clarify **Risk Assessment Questions**; anonymous risk assessment is conducted via Poll Everywhere®; Risk IPT members review and certify the risk assessment results

5. Report

Strategy, Policy Coordination, and Innovation (SP&I) provides risk assessment results to the **Executive Risk Steering Committee** (ERSC) for concurrence for further consideration by the **Executive Steering Committee** (ESC)

*Risk IPT membership is made up of representation from all TSA Program Offices

Strategy, Policy Coordination, and Innovation (SP&I)
Enterprise Performance and Risk (EPR)

STRATEGY, POLICY COORDINATION AND INNOVATION

TSA MANAGEMENT DIRECTIVE No. 4101
ENTERPRISE RISK MANAGEMENT

To enhance mission performance, TSA is committed to promoting a culture founded on its values of Integrity, Respect and Commitment.

REVISION:
This revised directive supersedes TSA MD 100.8, *Enterprise Risk Management*, dated October 22, 2014.

SUMMARY OF CHANGES:
Section 1, Purpose, updated contextual description; Section 3, added OMB Circular A-123 to authorities list; Section 4, Definitions, added Internal Controls, Key Performance Indicator (KPI), Risk Taxonomy, Operational (Mission) Risk, Risk Exposure, Risk Tolerance, Risk Profile, Risk Register, and Vulnerability. Updated Risk Appetite and Issue; Section 5, Responsibilities, added section dividers, Executive Assistant Administrators (EAAs), Risk Owners, and Program Offices; updated The Administrator, Chief Risk Officer (CRO), Assistant Administrators (AAs), ERM Program Office, Leadership Council (LC), and Risk Integrated Project Team (IPT); removed TSA Program Office ERM Liaisons; added Governance Bodies; added ERM Governance model (appendix A); Section 6, Policy, adapted duties aligned to the Chief Risk Officer to reflect TSA's ERM Approach overall; added details on Key Risk Management Functions and Enterprise Integration; Section 7, added key activities aligned to a seven-step ERM framework and contextual details on the TSA ERM Manual.

1. PURPOSE:

This directive provides TSA policy and procedures for Enterprise Risk Management (ERM).

For TSA to carry out its transportation security mission and accomplish its strategic objectives, the agency must understand the threats and opportunities across the transportation system and manage both effectively. Enterprise Risk Management provides the framework and structure that aids federal managers in balancing risks and opportunities to enhance enterprise decision making and optimize performance.

A mature Enterprise Risk Management program integrates risk as a consideration in key management processes such as Strategic Planning, Programming, Budgeting and Execution (PPBE-S), Program Management, Internal Controls, and Policy Development.

2. SCOPE:

This directive applies to all TSA Program Offices and staff that oversee risk management functions and support the execution of ERM.

3. AUTHORITIES:

A. Office of Management and Budget (OMB) Circular A-11 Sections 270.24 – 270.29

B. OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control

4. DEFINITIONS:

A. Chief Risk Officer (CRO): An executive in charge of managing risks at the enterprise level. As of the publishing of this MD, the Strategy, Policy Coordination, and Innovation (SP&I) Executive Director performs the duties of the CRO in collaboration with the Requirements and Capabilities Analysis (RCA) Assistant Administrator.

B. Enterprise Risk Management (ERM): A comprehensive approach to risk management that engages organizational systems and processes together to improve the quality of decision making for managing risks that may hinder an organization's ability to achieve its objectives. ERM does not limit its approach to focus on a specific type of risk, but instead provides a framework to address TSA's full spectrum of risks in the most effective manner.

C. ERM Program Office: The TSA Program Office generally responsible for leading and overseeing the ERM process, as described in Section 5.H of this Directive. It is located in TSA SP&I.

D. Enterprise Risk Register: A repository of documented risks used to aid in the discussion, validation, tracking, and reporting of risks.

E. Executive Risk Steering Committee (ERSC): Governing body that retains overarching responsibility for defining strategy and managing risk at an enterprise level. The ERSC is chaired by the Executive Director of Strategy, Policy Coordination, and Innovation (SP&I) and composed of Assistant Administrators (AAs) from across TSA as the scope of TSA's risk management efforts is enterprise-wide.

F. Internal Controls: Processes implemented by an organization's oversight body, management, and other personnel that help to provide reasonable assurance that the objectives of the organization will be achieved through measures that promote accountability, compliance and fraud prevention.

G. Key Performance Indicators (KPIs): Measures that gauge an organization's overall performance connected to strategic, financial, and operational achievements.

H. Key Risk Indicators (KRIs): Measures that provide early signals of increasing risk exposures in various areas of the enterprise.

I. Leadership Council (LC): A senior forum chaired by the Administrator and comprised of the Deputy Administrator, the Chief of Staff, and the Executive Assistant Administrators.

J. Operational (Mission) Risk: The risk of loss resulting from inadequate or failed internal processes, people, and systems, or from external events. At TSA, this risk category describes risks associated with efforts to protect the nation's transportation systems (e.g. terrorist attack on an aircraft and the procurement of critical security capabilities).

K. Program Office: A subordinate element of a HQ office.

L. Risk: Potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and associated impacts.

M. Risk Appetite: The overall level of risk that the agency is prepared to accept in pursuit of its general or specific objectives. TSA has defined statements that establish high-level guidelines for the types and level of risk appropriate within the agency.

N. Risk Exposure: Measurement of potential future loss resulting from an uncertain event.

O. Risk Owner: Person or entity with the accountability and authority to manage a risk.

P. Risk Profile: A prioritized inventory of an organization's most significant risks.

Q. Risk Taxonomy: A comprehensive classification scheme of risk categories and subcategories to enable consistent identification and categorization of risk.

R. Risk Tolerance: Threshold used to measure acceptable risk exposure based on the application of quantified risk appetite.

S. Vulnerability: A weakness or gap within a system that has the potential to be exploited by an adversary in order to compromise a target.

5. RESPONSIBILITIES:

A. The Leadership Council (LC) is responsible for making final rulings on cross-functional critical TSA issues including risk management.

B. The Executive Risk Steering Committee (ERSC) is responsible for:

(1) Overseeing the development and implementation of processes used to identify, analyze, prioritize, and respond to risks across TSA including terrorism threats facing the entire transportation sector and non-operational risks that could impede TSA's ability to achieve its strategic objectives.

(2) Ensuring risks are managed to create value for the Nation in a manner consistent with established risk appetite and tolerance levels and provides recommendations along with the associated data and information to the LC for an informed decision.

C. The Chief Risk Officer (CRO) is responsible for:

(1) Overseeing the design, development, and implementation of the TSA ERM program.

(2) Advising the Administrator and Deputy Administrator on all risk matters that could impact TSA's ability to perform its mission.

(3) Setting enterprise-level KPIs and KRIs related to enterprise risk management.

D. Executive Assistant Administrators (EAAs) are responsible for:

(1) Sponsoring enterprise risks assigned through their positions on the LC.

(2) Implementing consistent risk management practices including but not limited to:

i. Approving ERSC recommendations for the Enterprise Risk Register.

ii. Prioritizing enterprise risks for resource allocation, decision-making, strategic planning processes.

E. Assistant Administrators (AAs) are responsible for:

(1) Serving as risk owners, when officially designated, in accordance with the ERSC Charter.

(2) Developing risk mitigation plans and reporting on progress at ERSC and LC meetings for those areas where the AA serves as risk owner.

(3) Ensuring that Program Offices adopt and follow the ERM framework and participate in enterprise-wide risk management efforts within their individual office.

(4) Aligning management control techniques to risks as appropriate and ensuring these techniques are integrated into the Management Control Objective Plan (MCOP) program.

(5) Implementing consistent risk management practices in alignment with this directive.

(6) Applying enterprise-level risk appetite statements to set office-specific risk limits, where applicable.

(7) Developing and monitoring office-level KPIs and KRIs.

F. Risk Integrated Project Team (IPT) is responsible for sharing information and coordinating enterprise risks and security vulnerabilities and for developing an ERSC communications plan and elevating any material that contains risk related items to the ERSC.

G. ERM Program Office is responsible for:

(1) Leading ERM activities, including all related ERSC activities.

(2) Developing and maintaining ERM policies, processes, procedures, tools, and information systems.

(3) Leading efforts to perform enterprise risk identification, analysis, prioritization, and response.

(4) Overseeing the process for establishing ERM communication at all levels for gathering data and developing risk reports.

(5) Coordinating with program offices.

(6) Coordinating with other risk management partners (e.g. Aviation Security Advisory Committee, Surface Transportation Security Advisory Committee, Aviation Risk Management Working Group, etc.) as necessary in executing integrated ERM activities.

6. POLICY:

A. An integrated Enterprise Risk Management approach optimizes TSA's ability to respond to the complex challenges that come with adding security to the global transportation network, while helping TSA capitalize on opportunities to outpace and outmatch adversaries.

B. The TSA enterprise depends on a structured, disciplined, and consistent Enterprise Risk Management approach to identify, analyze, prioritize, and respond to risks in accordance with U.S. Department of Homeland Security guidance.

C. Recurring identification of risks that threaten TSA's achievement of long-term objectives and management of those risks at the enterprise level provides greater transparency, increases awareness of where risks are present and at what level within the organization they should be addressed, and enhances TSA's overall capability to respond to, monitor, and communicate risks.

D. The application of Enterprise Risk Management informs preparedness, planning, and resourcing in advance of and in response to a risk which warrants TSA, or as applicable DHS-wide, response due to the scale or scope of potential impact (how large and cross-cutting the risks are, respectively).

E. All staff shall adopt the principles of risk management developed through the Enterprise Risk Management program, and apply the standards, tools, and techniques in execution of their duties.

F. Though these activities are executed at different levels of the agency and under the authority of different offices (SP&I, RCA, etc.), interdependent and interconnected risk management efforts shall be integrated to foster an effective Enterprise Risk Management program.

G. Management processes enterprise-wide shall integrate risk management to enable optimized results. It is important that the following processes, incorporate risk management in particular:

(1) Strategic Planning;

(2) Planning, Programming, Budgeting, Execution, and Strategy (PPBE-S);

(3) Capability Management;

(4) Program Management;

(5) Policy Development; and

(6) Internal Controls.

7. PROCEDURES:

The execution of Enterprise Risk Management can be represented through a seven-step framework with key enterprise activities taking place in each step. ERM stakeholders should reference the *TSA ERM Manual,* which covers governance, collaborative activities, identification/mitigation processes, and other useful information in more detail.

A. Establish the Context (Step 1): Understand and articulate the internal and external environment of the organization. During this step, the Program Office defines their objectives, evaluate the external and internal parameters to be considered when managing risk, make changes to the risk management process, and develop risk criteria.

B. Identify Risks (Step 2): Identify enterprise-level risks to be managed by leveraging the Enterprise Risk Register. This process specifies what risks can occur, as well as where, when, why, and how they may occur. The list of risks identified through this process is preliminary and subject to further qualification and refinement as part of the Analyze Risks process.

C. Analyze Risks (Step 3): Analyze the causes and sources of a risk, the probability that the risk event will occur, magnitude and consequences of the event, and the likelihood that those consequences will be realized. Risk analysis provides the basis for evaluation and decisions regarding risk response. Each risk identified during the Identify Risks process is subjected to a qualitative evaluation of its likelihood and impacts. The list of risks is then narrowed and refined based on criteria approved by the ERSC. Those risks falling below a defined threshold may continue to be monitored and managed within TSA but will not be reported at the executive level in the Enterprise Risk Register.

D. Evaluate Risks (Step 4): Prioritize enterprise level risks using the qualitative risk analysis generated earlier. The prioritization of the enterprise-level risks enables TSA leadership response in the Respond to Risks process.

E. Respond to Risks (Step 5): Assess the range of risk response options and prepare implementation plans for selected response options. Responding to risks includes both taking advantage of opportunities to enhance mission success as well as efforts to minimize the adverse impacts of risks. A prioritized and quantified list enables TSA leadership in making informed strategic decisions about how to allocate resources.

F. Monitor and Review (Step 6): Conduct ongoing review of risk management efforts and response strategies to ensure that they remain relevant and effective. Factors that may affect the likelihood and consequences of an outcome may change over time, as may the factors that affect the suitability or cost of the selected response options. As a result, it is pertinent that this cycle continuously repeats. The Monitor and Review step also involves benchmarking definable ERM risk management outcomes against target or required performance levels.

G. Communicate and Consult (Step 7): Leverage existing channels to escalate risk information to senior leadership in order to obtain their feedback and guidance as appropriate. Clear communication channels are essential to fully integrating risk management across all relevant programs and to developing a culture where both positive and negative dimensions of risk are regularly discussed and valued.

8. APPROVAL AND EFFECTIVE DATE: This policy is approved and effective the date of signature unless otherwise specified.

APPROVAL

Signed May 5, 2022

_________________________ _________________________

[redacted]
Executive Director for
Strategy, Policy Coordination and Innovation

Date

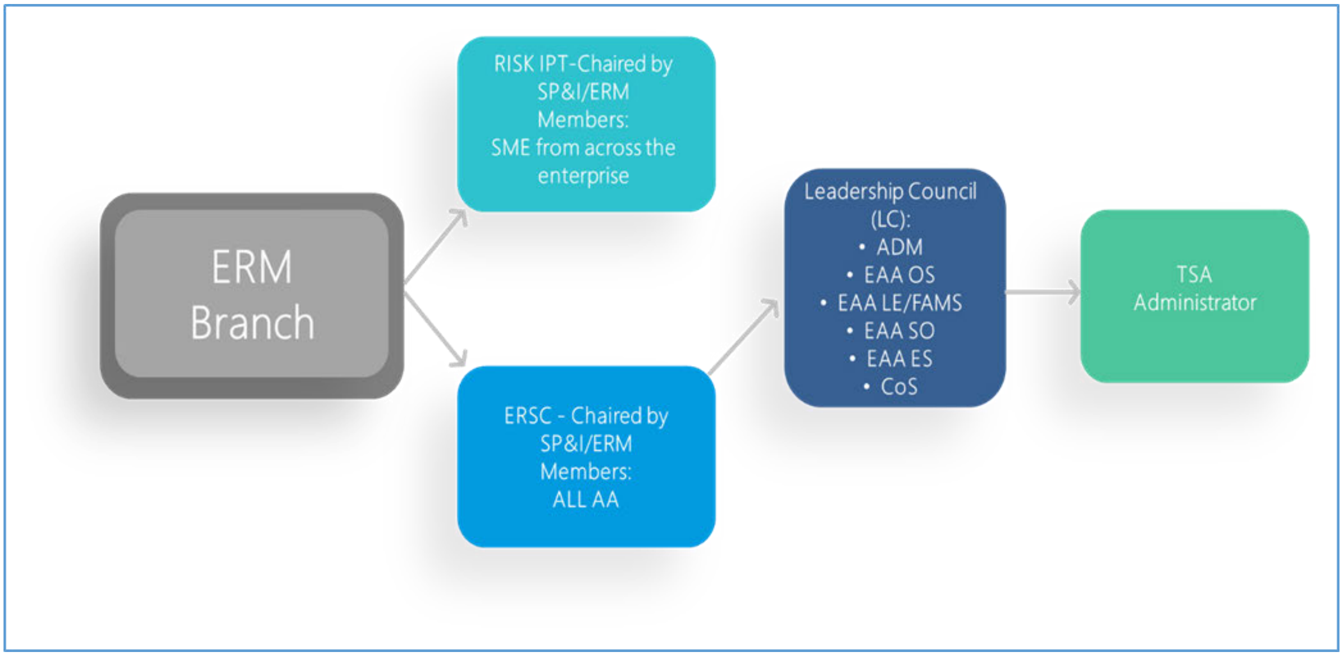
EFFECTIVE

____
Date

Distribution: All TSA
Point-of-Contact: Enterprise Risk Management Program Office, [redacted]

Appendix A

TSA ERM Governance Model


ERM Branch
RISK IPT-Chaired by SP&I/ERM Members: SME from across the enterprise
ERSC - Chaired by SP&I/ERM Members: ALL AA
Leadership Council (LC):
• ADM
• EAA OS
• EAA LE/FAMS
• EAA SO
• EAA ES
• CoS
TSA Administrator