



**U.S. OFFICE OF SPECIAL COUNSEL**  
**1730 M Street, N.W., Suite 300**  
**Washington, D.C. 20036-4505**

**The Special Counsel**

July 20, 2023

The Honorable Alejandro Mayorkas  
Secretary  
United States Department of Homeland Security  
2707 Martin Luther King, Jr. Ave. SE  
Washington, D.C. 20528-0525

Re: OSC File No. DI-23-000586  
Referral for Investigation—5 U.S.C. § 1213(c)

Dear Secretary Mayorkas:

I am referring to you for investigation a whistleblower disclosure of a substantial and specific danger to public safety at the U.S. Department of Homeland Security (DHS), Transportation Security Administration (TSA), Boston, Massachusetts. A report of your investigation of these allegations and any related matters is due to the Office of Special Counsel (OSC) on September 18, 2023.

Mr. [REDACTED], a Transportation Security Manager, who consented to the release of his name, reported allegations of malfunctioning security screening equipment at Boston Logan International Airport (Boston Logan). The allegations to be investigated include:

- The Advanced Imaging Technology (AIT) machines at Boston Logan failed to detect known security threats during TSA officer training exercises;
- Boston TSA management and the Boston Federal Security Director (FSD) failed to investigate these potential security vulnerabilities; and
- Any additional or related allegations of wrongdoing discovered during the investigation of the foregoing allegations.

Mr. [REDACTED] disclosed that the AIT machines, the primary security screening equipment at Boston Logan, failed to detect [REDACTED] materials during a TSA officer training exercise on March 11, 2023. Specifically, he observed that each of the three AIT units in Terminal E failed to alert when Lead Transportation Security Officer (LTSO) [REDACTED], using a "test kit" of [REDACTED] distributed for TSA officer training purposes, proceeded through the machines with [REDACTED]. Following the March 11 exercise, two of Mr. [REDACTED]'s colleagues, Supervisory Transportation Security Officers (STSOs) [REDACTED] and [REDACTED], reported that a similar malfunction of the AIT machines had been observed on March 3, 2023, during an exercise in which a TSA officer in the Boston Field Evaluation Training (BOS FET) Program [REDACTED] [REDACTED] and proceeded through the AIT machines in Terminal E without alert.

July 20, 2023


Page 2

Further, after Mr. [REDACTED] reported the observed malfunctions within his chain of command, Boston TSA management and the Boston Deputy Federal Security Director appointed a factfinder to conduct an informal Administrative Inquiry in accordance with TSA Management Directive 700.2.<sup>1</sup> However, Mr. [REDACTED] reported that the administrative inquiry did not address the underlying security concerns presented by the potentially malfunctioning screening equipment, but rather, was specifically limited to the question of whether the involved officers engaged in “unauthorized testing” of the AIT machines. To date, Mr. [REDACTED] has received no further information from TSA personnel in response to his report of the potential security vulnerabilities described above. Moreover, Mr. [REDACTED] maintains that the observed malfunctions occurred in the course of a routine TSA officer training exercise and not during any testing of the AIT machines.

Pursuant to my authority under 5 U.S.C. § 1213, I have concluded that there is a substantial likelihood that the information provided to OSC discloses a substantial and specific danger to public safety. Please note that specific allegations and references to violations of law, rule, or regulation are not intended to be exclusive. If, in the course of your investigation, you discover additional violations, please include your findings on these additional matters in the report to OSC. As previously noted, your agency must conduct an investigation of these matters and produce a report, which must be reviewed and signed by you. Per statutory requirements, I will review the report for sufficiency and reasonableness before sending copies of the agency report, along with the whistleblower’s comments and any comments or recommendations I may have, to the President and congressional oversight committees and making these documents publicly available.

Additional important requirements and guidance on the agency report are included in the attached Appendix, which can also be accessed at <https://osc.gov/Pages/DOW.aspx>. If your investigators have questions regarding the statutory process or the report required under 5 U.S.C. § 1213, please contact Catherine A. McMullen, Chief, Disclosure Unit, at (202) 804-7088 or [cmcmullen@osc.gov](mailto:cmcmullen@osc.gov) for assistance. I am also available for any questions you may have.

Sincerely,



Henry J. Kerner  
*Special Counsel*

Enclosure

cc: The Honorable Joseph V. Cuffari, Inspector General

---

<sup>1</sup> TSA Management Directive 700.2, *Informal Administrative Inquiries*, establishes TSA’s policies, requirements, and procedures for conducting informal administrative inquiries pertaining to TSA operations, including potential security violations.

## **APPENDIX**

### **AGENCY REPORTS UNDER 5 U.S.C. § 1213**

#### GUIDANCE ON 1213 REPORT

- OSC requires that your investigators interview the whistleblower at the beginning of the agency investigation when the whistleblower consents to the disclosure of his or her name.
- Should the agency head delegate the authority to review and sign the report, the delegation must be specifically stated and include the authority to take the actions necessary under 5 U.S.C. § 1213(d)(5).
- OSC will consider extension requests in 60-day increments when an agency evidences that it is conducting a good faith investigation that will require more time to complete.
- Identify agency employees by position title in the report and attach a key identifying the employees by both name and position. The key identifying employees will be used by OSC in its review and evaluation of the report. OSC will place the report without the employee identification key in its public file.
- Do not include in the report personally identifiable information, such as social security numbers, home addresses and telephone numbers, personal e-mails, dates and places of birth, and personal financial information.
- Include information about actual or projected financial savings as a result of the investigation as well as any policy changes related to the financial savings.
- Reports previously provided to OSC may be reviewed through OSC's public file, which is available here: <https://osc.gov/Pages/Resources-PublicFiles.aspx>. Please refer to our file number in any correspondence on this matter.

#### RETALIATION AGAINST WHISTLEBLOWERS

In some cases, whistleblowers who have made disclosures to OSC that are referred for investigation pursuant to 5 U.S.C. § 1213 also allege retaliation for whistleblowing once the agency is on notice of their allegations. The Special Counsel strongly recommends the agency take all appropriate measures to protect individuals from retaliation and other prohibited personnel practices.

#### EXCEPTIONS TO PUBLIC FILE REQUIREMENT

OSC will place a copy of the agency report in its public file unless it is classified or prohibited from release by law or by Executive Order requiring that information be kept secret in the interest of national defense or the conduct of foreign affairs. 5 U.S.C. § 1219(a).

#### EVIDENCE OF CRIMINAL CONDUCT

If the agency discovers evidence of a criminal violation during the course of its investigation and refers the evidence to the Attorney General, the agency must notify the Office of Personnel Management and the Office of Management and Budget. 5 U.S.C. § 1213(f). In such cases, the agency must still submit its report to OSC, but OSC must not share the report with the whistleblower or make it publicly available. See 5 U.S.C. §§ 1213(f), 1219(a)(1).