

Under § 1540.117(f), the Deputy Administrator reviews the Initial Notification of Threat Assessment, the materials upon which the Initial Notification was based, the individual's reply, if any, and any other materials or information available to him. The Deputy Administrator will undertake a *de novo* review to determine whether the individual poses a security risk.

If the Deputy Administrator determines that the individual poses a security threat, TSA serves upon the individual a Final Notification of Threat Assessment and serves a copy upon the Administrator. The Final Notification includes a statement that the Deputy Administrator has personally reviewed the Initial Notification, the individual's reply, if any, and any other materials or information available to him, and has determined that the individual poses a security threat. This Final Notification will form the basis of the FAA's revocation of, or denial of, the individual's certificate, rating, or authorization.

If the Deputy Administrator does not determine that the individual poses a security threat, TSA serves upon the individual a Withdrawal of the Initial Notification and serves a copy upon the FAA.

Section 1540.117(g) provides that in connection with this section, TSA does not disclose to the individual classified information, as defined in Executive Order 12968 section 1.1(d), and TSA reserves the right not to disclose any other information or material not warranting disclosure or protected from disclosure under law, such as sensitive security information (SSI), sensitive law enforcement and intelligence information; sources, methods, means, and application of intelligence techniques, and identities of confidential informants, undercover operatives, and material witnesses.

In most cases, the determination that an individual poses a security threat will be based, in large part or exclusively, on classified national security information, unclassified information designated as SSI, or other information that is protected from disclosure by law, such as the Freedom of Information Act (FOIA). See 5 U.S.C. 552(b)(1), (2), (7).

Classified national security information is information that the President or another authorized Federal official has determined, pursuant to Executive Order (EO) 12958, must be protected against unauthorized disclosure in order to safeguard the security of American citizens, the country's democratic institutions, and America's participation within the

community of nations. See E.O. 12958 (60 FR 19825, April 20, 1995). E.O. 12968 prohibits Federal employees from disclosing classified information to individuals who have not been cleared to have access to such information under the requirements of that EO. See E.O. 12968 sec. 3.2(a), 6.2(a)(1) (60 FR 40245, Aug. 7, 1995). If the Assistant Administrator has determined that an individual who is the subject of a threat assessment proceeding poses a threat to transportation security, that individual will not be able to obtain a clearance to have access to classified national security information, and TSA has no authority to release such information to that individual.

The denial of access to classified information under these circumstances is consistent with the treatment of classified information under the FOIA, which specifically exempts such information from the general requirement under FOIA that all government documents are subject to public disclosure. See 5 U.S.C. 552(b)(1).

SSI is unclassified information that is subject to disclosure limitations under statute and TSA regulations. See 49 U.S.C. 114(s); 49 CFR part 1520. Under 49 U.S.C. 114(s), the Under Secretary may designate categories of information as SSI if release of the information would be detrimental to the security of transportation. The SSI designation allows TSA to limit disclosure of this information to people with a need to know in order to carry out regulatory security duties. See 49 CFR 1520.5(b).

Among the categories of information that the Under Secretary has defined as SSI by regulation is information concerning threats against transportation. See 49 CFR 1520.7(i). Thus, information that TSA obtains indicating that an individual poses a security threat, including the source of such information and the methods through which the information was obtained, will commonly be SSI or classified information. The purpose of designating such information as SSI is to ensure that those who seek to do harm to the transportation system and their associates and supporters do not obtain access to information that will enable them to evade the government's efforts to detect and prevent their activities. Disclosure of this information, especially to an individual specifically suspected of posing a threat to the aviation system, is precisely the type of harm that Congress sought to avoid by authorizing the Under Secretary to define and protect SSI.

Other types of information also are protected from disclosure by law due to

their sensitivity in law enforcement and intelligence. In some instances, the release of information about a particular individual or his supporters or associates could have a substantial adverse impact on security matters. The release of the identities or other information regarding individuals related to a security threat determination by TSA could jeopardize sources and methods of the intelligence community, the identities of confidential sources, and techniques and procedures for law enforcement investigations or prosecution. See 5 U.S.C. 552(b)(7)(D), (E). Release of such information also could have a substantial adverse impact on ongoing investigations being conducted by Federal law enforcement agencies, possibly giving a terrorist organization or other group a roadmap of the course and progress of an investigation. In certain instances, release of information could alert a terrorist's coconspirators to the extent of the Federal investigation and the imminence of their own detection, thus provoking flight. Those without access to information about the progress of federal investigations are not in a meaningful position and therefore cannot make judgments about the risk of release of information about that investigation that TSA has relied upon in making a security threat determination.

This intelligence "mosaic" dilemma has been well recognized by the courts in concluding both that they are ill-suited to second guess the Executive Branch's determination and that seemingly innocuous production should not be made. The business of foreign intelligence gathering in this age of computer technology is more akin to the construction of a mosaic than it is to the management of a cloak-and-dagger affair. Thousands of pieces of seemingly innocuous information can be analyzed and fitted into place to reveal with startling clarity how the unseen whole must operate. The Fourth Circuit Court of Appeals has observed:

"The significance of one item of information may frequently depend upon knowledge of many other items of information. What may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene and may put the questioned item of information in its proper context. The courts, of course are ill equipped to become sufficiently steeped in foreign intelligence matters to serve effectively in the review of secrecy classifications in this area."

*United States versus Marchetti*, 466 F. 2d 1309, 1318 (4th Cir.), cert. denied, 409 U.S. 1063 (1972). *Halkin versus Helms*, 598 F. 2d 1 (D.C. Cir. 1978). See