

EXHIBIT 18

~~FILED UNDER SEAL~~

U.S. Department of Homeland Security
U.S. Citizenship and Immigration Services
*Office of Fraud Detection and National
Security*
Washington, DC 20529



U.S. Citizenship
and Immigration
Services

Supplemental Guidance:

Revision of Responsibilities for CARRP Cases Involving Known or Suspected Terrorists

A. KST Hits

HQFDNS has issued a policy memo directing that external vetting for Known or Suspected Terrorists (KSTs) should now be done by local Field Offices and Service Centers. These questions and answers serve as supplemental guidance to clarify the requirements of the new CARRP policy, and answer questions raised during the drafting phase of the policy.

CARRP procedures and requirements outlined in existing policy and operational guidance (provided by various HQ directorates) remain the same, other than those specified in the attached policy memorandum. Also, this revised policy does not replace existing protocols, work flow process and procedures, or delineated roles and responsibilities of USCIS officers currently processing CARRP cases.

1. Who will conduct external vetting of KST cases?

External vetting of KST cases will now be conducted by those officers currently assigned to conduct external vetting for non-KST cases (i.e., FDNS IOs, Background Check Unit officers, and etc.).

2. How will field offices conduct external vetting if they do not have a designated USCIS representative with local JTTF?

To conduct external vetting, the field must have the contact name and phone number for the law enforcement agency (LEA) and/or record owner who may or may not be assigned to a local Joint Terrorism Task Force (JTTF). While having a designated USCIS representative with local JTTF is highly advantageous, it is not a necessary requirement for the field to be able to conduct external vetting.

Field offices that do not have an established relationship with their local JTTF or other Law Enforcement Intelligence Community (LEIC) partners may continue to request

assistance in identifying the record owner by submitting a Request for Assistance (RFA) to HQFDNS via the [REDACTED]@dhs.gov mailbox.

3. What is the difference between KST and Non-KST external vetting?

There is no difference. The purpose of external vetting, as defined in current operational guidance provided by various Directorates, is to make inquiries of record owners in possession of national security (NS) information. Specifically, the designated officer will determine the nature and quality of the NS concern, the status of any investigation related to the NS concern, and if the NS concern impacts the subject's eligibility for the benefit requested or if the alien may be subject to a ground of removal under the Immigration and Nationality Act (INA). Officers should note that actions that do not meet the threshold for criminal prosecution (e.g., indicators of fraud, foreign travel, and information concerning employment or family relationships) may be relevant to a benefit determination.

External vetting must be conducted if no ineligibility grounds have been identified (after eligibility assessment and internal vetting have been completed) or if Field Management determines further processing is necessary to strengthen or support a decision.

4. What is the purpose of Classified High Side Checks?

The purpose of classified checks is to obtain additional information that may identify additional ineligibility grounds or support additional lines of questioning. However, classified High Side checks must not be requested routinely. Rather, the field must articulate a need for such checks. For example, the field may request high side checks when the nominating agency is either a foreign entity or a member of Intelligence Community (other than the FBI) and additional information cannot be obtained through the local JTTF.

NOTE: In reviewing the classified systems check results to identify possible grounds of ineligibility, develop lines of questioning when interviewing the individual, or identify information which if declassified, could be used to support a denial, the field must never cite the information provided by another agency in a decision without first obtaining written permission from the originating agency. Additionally, the field should never develop a line of questioning or provide a written decision which could implicate classified information that has not been declassified unless it can be clearly demonstrated that the information can be obtained from a publicly available source. If the information has been declassified, the field must still obtain written permission from the originating agency to use the information. The field may request assistance from HQFDNS in declassifying information if the owner of the information requests HQ involvement.

5. Can the field approve KST cases?

No. Officers in the field are not authorized to approve KST cases. Current policies and procedures for the approval of cases involving KSTs have not been changed.

6. What should the field do with KST cases that have been determined to be otherwise approvable?

Upon completion of internal and external vetting, if the national security concern remains, or the KST individual remains eligible for the benefit, the KST case must be elevated to the respective HQ directorate point of contact (POC) for further evaluation, in consultation with local and HQ counsel.

HQ will return a case to the submitting officer when senior leadership and the USCIS Deputy Director have reviewed the application or petition and made an appropriate recommendation, or released the case to the field for adjudication.

7. How should the KST cases be elevated to respective HQ directorate?

Officers should follow current local and directorate guidance for forwarding cases to their respective HQ directorate POCs.

8. What will happen to the existing Request for Assistance (RFA) process?

HQFDNS is not changing the existing RFA process. However, the nature of assistance provided will be different.

Upon obtaining local management approval, the field may e-mail an RFA to HQFDNS (██████████@dhs.gov) under the following circumstances:

- To identify the NS record owner of the KST nominating entity;
 - HQFDNS will identify a POC. The field must then contact the POC for external vetting and deconfliction.
 - If HQFDNS is unable to identify a POC¹, HQFDNS will conduct external vetting and deconfliction.
- To seek assistance in contacting or resolving issues with the record holder; and
- To conduct queries of classified systems.

¹ These KSTs are generally nominated by certain members of Intelligence Community for which a POC is not available.

9. *Can the field contact the record owner who is a member of the Intelligence Committee?*

Contact with the Intelligence Committee is not reserved for HQFDNS if the Intelligence Community member has released his/her name for the field to contact. If the name is not released or is not available, HQFDNS will conduct external vetting before returning the case back to the field.