

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY

Date: 11/17/2008

To: All Divisions

Attn: Executive Assistant Directors,
Assistant Directors,
ADICs,
SACs,
Legats,
Administrative Officers
SAS-Records
Records Liaisons
File Supervisors

From: Director's Office
RPO/CPO/Room 6248

Contact: [REDACTED]

Approved By: [REDACTED]

b6
b7C

Drafted By: [REDACTED]

Case ID #: 3190-HQ-A1487624-253

Title: RECORDS MANAGEMENT MATTERS;
RECORDKEEPING CHANGES RELATED TO THE
ATTORNEY GENERAL GUIDELINES FOR
DOMESTIC FBI OPERATIONS (AGG-DOM) AND
FBI DOMESTIC INVESTIGATIONS AND
OPERATIONS GUIDE (DIOG)

Synopsis: To advise recipients of necessary modifications to pending "threat assessment" files based upon the transition to the new AGG-Dom and the DIOG. Additionally, this Electronic Communication (EC) provides recipients information regarding existing Preliminary and Full investigation cases opened under the investigative classifications. This communication has been coordinated with the Records Management Division (RMD).

Reference: 319W-HQ-A1487698-DO Serial 9

Administrative: This Electronic Communication (EC) is one of many communications issued as part of the transition to the new AGG-Dom. The objective of these communications is to educate the

To: All Divisions From: Director's Office
Re: 3190-HQ-A1487624, 11/17/2008

workforce, or a segment thereof, on meeting the new requirements for implementing those guidelines. This EC is specifically focused on file management changes and recordkeeping practices that will affect **Program Managers, Administrative Officers, File Supervisors, Records Liaison Officers, and Support Service Technicians (SST)**.

Enclosure(s): Enclosed is an ACS report with all cases, regardless of case type (i.e. control, administrative or investigative) with the words "Threat Assessment" in the title.

Details: The implementation of the Attorney General's Guidelines for Domestic FBI Operations (AGG-Dom) will be undertaken through the FBI's Domestic Investigations Operations Guide (DIOG), which will govern FBI operational activities effective 12/01/2008. Since the AGG-Dom has new information collection and reporting requirements adopted by the DIOG, the FBI must modify its recordkeeping procedures to conform with these mandates.

The AGG-Dom combines "threat assessments" under the former Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection and the "prompt and extremely limited checking of initial leads" under the former Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations into a new investigative category entitled "Assessments." Under the DIOG, all Assessments must either be opened in an investigative classification as an Assessment file or placed in a To transition to this new process, current FBI threat assessment files must be reviewed to determine how they should be managed under the new DIOG procedures.

b7E

Consequently, the Corporate Policy Office (CPO), in coordination with ITOD, has identified a number of cases in ACS, captioned "Threat Assessments," that must be updated. Therefore, the following steps should be undertaken upon receipt of this communication:

- By 11/30/2008, offices should:
 1. Identify files (control, administrative or investigative) used for threat assessments (see enclosure).

To: All Divisions From: Director's Office
Re: 3190-HQ-A1487624, 11/17/2008

2. Review your office's cases identified as threat assessment and determine if cases are actually filed properly.
3. For those determined to be threat assessment cases, determine what type of assessments are kept in the files by dividing the cases into two categories:
 - a. Prompt checking of leads, threat incidents or response to complaints
 - b. Threat assessments having a strategic, Domain Management or Special Events focus
4. For those determined not to be threat assessment cases, determine if case should remain open under another file classification, or closed if no longer needed.
 - a. Administrative files - Use the appropriate 319 file for administrative matters

By 12/12/2008, offices should:

1. Administratively close (C4) the files identified as threat assessment cases.
2. Maintain (i.e. serialize) "prompt checking of lead or threat incident" assessments in the appropriate [redacted] (i.e. [redacted])b7E
3. Reopen "strategic, Domain, or Special Event type threat assessments as Assessment files, and ensure that:
 - a. The source code is changed to 12
 - b. The Assessment Purpose is entered in the Summary field
 - c. The current date is entered in the Assessment Begin field

Currently, Guardian is used for International Terrorism Threat Incidents/Assessments and classification 324 is used to manage these records. Upon the implementation of the DIOG, classification 324 will be inactivated by FBIHQ. Field offices

To: All Divisions From: Director's Office
Re: 3190-HQ-A1487624, 11/17/2008

will then use the appropriate 315 zero sub-assessment file to manage their Guardian records. Several field offices have pending 324 files. These files must be reviewed as follows:

By 11/30/2008, offices should:

- Identify their office's pending 324 files and the type of information maintained in these files.

By 12/12/2008, offices should:

1. Identify their office's pending 324B (Potential Nexus to Terrorism) files and ensure that Threat Assessment information related to terrorism which is still subject to investigative activity is maintained in Guardian.
2. Administratively close (C4) the 324B file. All terrorism related threat information must be entered into Guardian. When the matter is cleared in Guardian, it will be maintained (i.e. serialized) in the appropriate [redacted] (i.e. [redacted] or if sufficient information is developed, it will be used to open a predicated case.
3. If the 324B file was inappropriately classified and should have been opened as a predicated file, reclassify the 324B into the appropriate investigative classification.
4. Identify their office's pending 324A (Unknown Nexus to Terrorism) files and review to determine if they contain information related to terrorism which is still subject to investigative activity.
5. If the 324A files do contain information related to terrorism which is still subject to investigative activity, then ensure that the information is maintained in Guardian.
6. Administratively close (C4) the 324A file. All terrorism related threat information must be entered into Guardian. When the matter is

b7E

To: All Divisions From: Director's Office
Re: 3190-HQ-A1487624, 11/17/2008

cleared in Guardian, it will be maintained
(i.e. serialized) in the appropriate [redacted]
[redacted] (i.e. [redacted])
or if sufficient information is developed, it
will be used to open a predicated case.

b7E

7. If the 324A file was inappropriately classified, it should be reclassified into the appropriate investigative classification.

For information of the recipients, the following modifications to ACS will be made upon the implementation of the DIOG:

- All cases opened within the investigative classifications will have to be identified as one of four investigative categories, i.e. Assessment, Preliminary Investigation (PI), Full, or Enterprise.
- All cases must have a begin date associated with the Assessment, PI, Full, or Enterprise initiation.
- On 12/1/2008, all pending investigative files not already designated as PI or Full investigations will be identified as Full investigations, with the begin date as the date the case was opened.

For file managers, additional details on the manner ACS will capture information is as follows:

- Existing Preliminary Investigation (PI): PI begin and PI deadline dates will be moved to the PI BEGIN and PI DEADLINE fields in the "Issue/Country/Investigative Category Dates" window
- Existing Full Investigation (FI): Full begin date will be moved to the FULL BEGIN field in the "Issue/Country/Investigative Category Dates" window
- Existing PI cases that were converted to FI: PI Begin, PI deadline, and Full begin dates will be moved to the PI BEGIN, PI DEADLINE, and FULL BEGIN fields in the "Issue/Country/Investigative Category Dates" window
- Existing cases without a PI or FI begin date: Cases will be identified as Full investigation in ACS, and

To: All Divisions From: Director's Office
Re: 3190-HQ-A1487624, 11/17/2008

the date the case was opened will be moved to the FULL
BEGIN field in the "Issue/Country/Investigative
Category Dates" window.

The table below displays the volume of cases opened in
the investigative classifications. For the list of investigative
classifications see



b7E

TABLE 1: Investigative Cases

CASE CHARACTERISTICS				
Preliminary Investigation (PI)				
Preliminary Investigation (PI)				
Full Investigation (FI)				
Full Investigation (FI)				
Preliminary Investigations converted to Full Investigations				
Preliminary Investigations converted to Full investigations				
Not identified as Preliminary Investigation/Full Investigation				
Not identified as Preliminary Investigation/Full Investigation				
All cases				

b7E

To: All Divisions From: Director's Office
Re: 3190-HQ-A1487624, 11/17/2008

All cases				
Grand Total				

b7E

To: All Divisions From: Director's Office
Re: 3190-HQ-A1487624, 11/17/2008

LEAD(s):

Set Lead 1: (Action)

ALL RECEIVING OFFICES

Identify and review all existing threat assessment cases and classification 324 cases by COB 11/30/2008.

Set Lead 2: (Action)

ALL RECEIVING OFFICES

Close threat assessment and classification 324 cases and follow instructions detailed above by COB 12/12/2008.

♦♦

