DEPARTMENT OF THE ARMY
UNITED STATES ARMY INTELLIGENCE AND SECURITY COMMAND
FREEDOM OF INFORMATION/PRIVACY OFFICE
FORT GEORGE G. MEADE, MARYLAND 20755-5995

REPLY TO
ATTENTION OF:

Freedom of Information/
Privacy Office

AUG 24 2009

Ms. Marcia Hofmann
Electronic Fronteir Foundation
1875 Connecticut Avenue, Northwest
Suite 650
Washington, DC 20009

Dear Ms. Hofmann:

This is in further response to your Freedom of Information Act (FOIA) request of November 15, 2006, for records relating to "TALON" reports and supplements our response of July 9, 2009.

Coordination has been completed and the records have been returned to this office for our disposition. We have reviewed the records and determined the records are releasable to you. The records are enclosed for your use.

There are no assessable FOIA fees for processing this request.

If you have any questions regarding this action, feel free to contact this office at 1-866-548-5651 (Press 2/Press 6), or email the INSCOM FOIA office at: INSCOM_FOIA_Service Center@mi.army.mil and refer to case #542F-09.

Sincerely,

Susan J. Butterfield
Director
Freedom of Information/Privacy Office
Investigative Records Repository

Enclosure

Enclosure (1) to Deputy Chief of Staff, G-2 Memorandum, "Interim Implementation Guidance for Army Intelligence and Counterintelligence Activities Regarding TALON Reporting"

ARMY INTERIM TALON IMPLEMENTATION GUIDANCE

1. (U) Reporting TALON Information.

a. (U//FOUO) Agency Review Process: The report drafter (Agent) will compose a new TALON report and save it as a draft TALON in the template provided in a restricted queue on the Cornerstone database web page. The report will include the mandatory fields identified on the template and a comment field that will require the reporting agency's reviewer's authorization. Army counterintelligence and intelligence activities will establish an internal review process for TALONs. Once this review is annotated on the template, the draft will then be ready for review by the Counterintelligence Field Activity (CIFA) and released to the Cornerstone database by CIFA. The Army Counterintelligence Information Center (ACIC) will establish specific guidelines for submission by US Army Military Intelligence (MI) activities of TALONs with US person information.

(1) (U//FOUO) This process will allow for the reporting agency, and the ACIC, 902d MI Group to review all TALON reports containing US person information submitted by Army MI activities prior to their release to the CIFA Cornerstone database. The ACIC is the only Army MI activity authorized to release TALON reports containing US person information to CIFA for inclusion in the Cornerstone database.

(2) (U//FOUO) Release Authority (CIFA): CIFA will be the final release authority for TALON reporting into the Cornerstone database.

b. (U//FOUO) Information about a possible international terrorist threat that is sufficiently credible to warrant an investigation must be referred to the proper investigative agency immediately, in addition to reporting via the TALON reporting system. Access to that report will be restricted to users with a need-to-know.

c. (U//FOUO) Information that is reportable under the provisions of AR 381-12 will be reported into SAEDA channels. Information that is responsive to intelligence or counterintelligence standing collection requirements will be reported in Intelligence Information Reports and will not be entered into the TALON Reporting System.

d. (U//FOUO) Organizations reporting TALON information must have a reasonable belief that there is a nexus between the information and "international terrorist activity" that may pose a threat to DoD personnel or resources.

e. (U) Criteria for TALON reporting.

(1) (U//FOUO) Specific or nonspecific threats to DoD interests.

(2) (U//FOUO) Suspected surveillance of DoD facilities or personnel.

(3) (U//FOUO) Elicitation attempts, suspicious questioning, or other suspected intelligence collection activities focused on DoD interests.

(4) (U//FOUO) Tests of security.

(5) (U//FOUO) Unusual repetitive activity.

(6) (U//FOUO) Bomb threats.

(7) (U//FOUO) Any other suspicious activity and incidents reasonably believed to be related to international terrorist activity directed against DoD personnel, property, and activities within the United States or abroad.

(U) Note: Although this program is focused on DoD facilities, interests or personnel, should nonspecific information be received about suspicious activities possibly linked to international terrorist actions against non-DoD personnel, activities or facilities, that information should be provided to the appropriate locally affected command and law enforcement (LE) authorities.

f. (U) TALON reports will not be used to report on US persons exercising their constitutionally protected freedoms of speech and assembly.

2. (U) Retention of TALON reports by Army Intelligence and Counterintelligence activities:

a. (U) No Army MI asset **(including the ACIC)** will maintain an internal TALON database.

b. (U) The ACIC is the only Army intelligence asset authorized to maintain information **gleaned** from TALON reports. The ACIC may retain information **gleaned** from TALON reports for as long as necessary for analytic purposes; however, if a TALON report contains identifying US person information the following applies:

(1) (U) Identifying US person information in TALON reports may be retained as long as necessary if there is a reasonable belief the person is engaged in or about to engage in international terrorist activities.

(2) (U) If this reasonable belief cannot be established within 90 days from the time the information is reported by the Army MI activity, the ACIC must notify CIFA to delete the TALON report containing US person information.

c. (U) The ACIC will immediately notify Army MI activity reporters whether any TALON reports containing US person information will be removed from the TALON database.

3. (U) Interaction between Army MI and LE entities concerning TALON reportable information:

a. (U) Army LE entities (MP/CID field elements) that acquire any possible TALON related information will input the information into the Joint Protection Enterprise Network system (JPEN) and also pass any TALON reports with US person information to the local MI elements for information purposes.

b. (U) Other information acquired by LE entities that does not meet the TALON criteria as outlined in paragraph 1e, will be processed according to LE entities' internal procedures.

c. (U) ACIC analysts will review all reports prior to submission to the TALON Cornerstone database. Any report that is determined to be law enforcement or domestic extremist related rather than international terrorist related will not be entered into the TALON Cornerstone database; however, the report will be given to the CID agent assigned to the ACIC for processing through LE channels.

d. (U) At all levels, information acquired by MI organizations that is of LE interest will be passed to LE authorities through established channels.

e. (U) When the creator of a TALON report identifies possible terrorist activity he will immediately notify his superior who will in turn notify law enforcement agencies, command authorities and CIFA.

f. (U) When the ACIC identifies possible terrorist activity through analysis, the ACIC will immediately notify law enforcement agencies, command authorities and CIFA.

4. (U) Intelligence oversight training. All Army intelligence and intelligence support assets who submit, process, and coordinate TALON reports will conduct annual training focused on the policies and procedures regarding collection, retention, and dissemination of US Persons information.

DEPARTMENT OF THE ARMY
OFFICE OF THE DEPUTY CHIEF OF STAFF, G-2
Responses to DoD Integrated Threat Working Group Task

USDI Integrated Threat Working Group Task

Task: Identify issues concerning the current DoD TALON policy and provide recommendations to those issues.

(1) Issue: Ambiguities in linking the criteria to a nexus to international terrorism.

- Although the 30 Mar 06 DEPSECDEF memorandum, subject: "Threats to the Department of Defense" stipulates that TALON reports must have a nexus to international terrorism, and defines those activities that may be reported as having a nexus to international terrorism solely because they meet the criterion listed in the memorandum causes confusion in the field.

- DEPSECDEF memorandum states: If information meets the following criteria (Specific or non-specific threats; surveillance; elicitation; Test of security; Repetitive activities; Bomb threats; Suspicious activities/incidents), the reporting organization is deemed to hold a reasonable a reasonable belief that there is a nexus between the information and international terrorism activity.

- As an example: A Fort Belvoir school bus full of kids taking pictures of Fort Belvoir probably does not constitute a foreign nexus (although the ambiguities in the language of the DEPSECDEF memorandum says it does) but some "tourists" taking photos of Fort Belvoir could reasonably constitute a nexus.

Recommendation: The verbiage in enclosure 1 to the DEPSECDEF memorandum be changed to read: "If information meets the reporting criteria above, and there is a reasonable belief of trained law enforcement or military intelligence personnel that a nexus between the information and international terrorism activity could exist, it may be forwarded to CIFA as a TALON report for inclusion in the Cornerstone database."

(2) Issue: Sharing Information between reporting mechanisms

- Currently law enforcement (LE) entities report TALON information via the Joint Protection Enterprise Network ((JPEN) and Army Military Intelligence (MI) entities report TALON information via the

Cornerstone database. This especially applies to the Army because there is a true separation between LE and MI (Air Force and Navy bifurcate their information between the two systems.) The purpose of the TALON reporting system being two fold (1) collect, and share non-validated threat information between LE and MI, and (2) subject that information to careful analysis. The purpose of the TALON report is to document and immediately disseminate potential threat information.

- The JPEN is an unclassified system available for use by all Services; reports entered into this system are immediately available to all Services LE assets utilizing the system. This provides instantaneous sharing of threat information with all posts, bases, and facilities.

- The Cornerstone database is limited to those activities that have classified systems, which in-turn limits the dissemination of threat information. However, the Cornerstone database provides access to information on a system that can subject that information to careful analysis.

Recommendation: All elements who produce TALON reports (including Army MI) should utilize the JPEN for reporting purposes. This will allow for instantaneous sharing of potential threat information with all posts, bases, and facilities. For purposes of analysis, CIFA would extract data from JPEN that meets the criteria for TALON reports and transfer that information to the Cornerstone database.

(3) Issue: Retention of Information Reported through the TALON System

- As per the 30 Mar 06, DEPSECDEF memorandum, TALON information will be retained per DODD 5240.1. This works well for information reported directly to the CIFA TALON Cornerstone database, however, this is not the case for information reported through the JPEN. NORTHCOM maintains a policy of purging all reports reported to JPEN at the 90-day point.

- Army LE entities (OPMG and CID) have both expressed concerns regarding the loss of information reported through the JPEN system. Although CIFA extracts reports from the JPEN that are deemed to meet TALON reporting criteria, not all reports will be extracted. However, NORTHCOM currently purges all data within JPEN that reaches the 90-day point. As a result, the data that is not captured by CIFA for inclusion in the Cornerstone database is lost. This information, although not specifically meeting TALON reporting criteria may be of use to the LE community.

Recommendation: USD(I) better define and promulgate guidance for the retention of information submitted to the JPEN.