NCTC POLICY DOCUMENT

Title: Information Sharing Rules of the Road

NCTC Policy Number: 1

1. Purpose:

A. To establish the policy by which NCTC personnel will share information with counterterrorism community partners.
B. This policy supersedes NCTC Policy 11.2.

2. References:

A. The National Security Act of 1947, as amended;
B. Intelligence Reform and Terrorism Prevention Act of 2004, as amended;
C. Executive Order (EO) 12333, United States Intelligence Activities, as amended;
D. EO 12968, Access to Classified Information, as amended;
E. EO 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans (Oct. 27, 2005);
F. EO 13526, Classified National Security Information (Jan. 5, 2010);
G. Intelligence Community Directive (ICD) 501, Discovery and Dissemination or Retrieval of Information within the Intelligence Community (Jan. 21, 2009);
H. Intelligence Community Policy Guidance (ICPG) 501.1, Exemption of Information from Discovery (May 26, 2009);
I. ICPG 501.2, Sensitive Review Board and Information Sharing Dispute Resolution Process (May 26, 2009);
J. ICPG 501.3 Subsequent Use of Information (May 20, 2010);
K. EO 13556, Controlled Unclassified Information (Nov. 4 2010); and
L. EO 13526 Guiding Principles for Use of the ORCON Marking and for Sharing Classified National Intelligence with U.S. Entities, March 2011.

1

3. Applicability:

This policy applies to all NCTC personnel including permanent cadre, detailees, assignees, and contractors (hereinafter "NCTC personnel").

4. Policy:

A. NCTC personnel must comply with all laws, EOs, and Attorney-General approved Guidelines with regard to their access, use, dissemination and retention of data.

B. NCTC personnel must also comply with all policies, principles, memoranda of understanding or agreement, and other agreements entered into by NCTC with another agency related to data access, use, dissemination, retention, deletion, feedback, classification and control markings, as well as any additional requirements imposed by the Office of the Director of National Intelligence (ODNI), the Director of the National Counterterrorism Center (D/NCTC), a data provider, or the United States Attorney General (AG). NCTC personnel may access information related to such requirements on NCTC Connect, or may contact the Information Sharing Program and Policy Office (ISPPO) with questions.

C. NCTC personnel may only access, use and disseminate information in furtherance of their official duties, and only through official channels. Access, use or dissemination of information for any other purposes, or through other than official channels, is strictly prohibited.

D. Detailees and assignees with access to information that they would otherwise not have access to at their home agencies are prohibited from sharing such information with their home agencies without express permission from the data originator and their NCTC Directorate leadership. Any approved sharing shall be done in accordance with NCTC policies and procedures.

E. NCTC personnel may not provide or discuss information related to operations or unfinished intelligence with other government agency's (OGA) employees outside of NCTC unless:
   1. The requesting OGA has received a copy of the same intelligence from the originating agency directly, or
   2. NCTC secured approval from the originating agency to provide the requested information to the OGA. This approval may be secured in advance, or as a blanket approval through a Memorandum of Agreement or Understanding between NCTC and OGAs.

F. Specific Types of Information.
   1. Sensitive Finished Intelligence (FININTEL) Coordination: NCTC maintains lists of officers from OGAs with which NCTC coordinates sensitive drafts of FININTEL. These lists are pertinent for the President's Daily Brief (PDB), National Terrorism

Bulletin (NTB), the Presidential Support and Production Group (PSPG), and the DNI Homeland Task Force Update. These lists are for FININTEL coordination only. They do not permit coordination of any unfinished intelligence that supports the FININTEL, unless permission from the unfinished intelligence originator has been received.

2. Non-Sensitive FININTEL Coordination: All products may be coordinated with individuals in the counterterrorism (CT) community with the appropriate clearances, and in the case of originator controlled (ORCON – may not be further disseminated in any way without explicit permission of the originating agency) FININTEL, with those agencies who received the ORCON source material through original distribution on the "to:" or "cc:" line.
3. Operational information: NCTC personnel must obtain permission from the originating agency for the passage of any operational reports or any information that may have operational or investigative significance to OGAs without exception.
4. Sensitive Source Reports (SSRPs): The coordination process for SSRPs is restricted to individuals read in to those programs.

G. Nothing in this policy shall be interpreted to restrict NCTC's statutory responsibility for ensuring that agencies, as appropriate, have access to and receive FININTEL and situation reports, as well as threat matrices to support their counterterrorism mission.
   1. NCTC personnel are free to share FININTEL regarding terrorism information to the limits of the classification and control markings associated with the information.
      a. For FOUO data, analysts can share terrorism information across the CT community. If FOUO data is shared electronically across the internet (e.g., AIN) it shall be encrypted. For Confidential, Secret and Top Secret NOFORN FININTEL, without other caveats, the terrorism information may be shared with appropriately cleared personnel.
      b. For ORCON FININTEL, the data may be shared with any agency that was on distribution for the original data, their subordinate components and/or any agency that is approved by the OGA, owning the OC.
      c. The NTB may be shared only with the by-name list of approved recipients.
   2. IC elements are authorized to share classified national intelligence information marked ORCON without further originator authorization in certain ODNI pre-approved collaborative secure environments, such as A-Space. This authorization applies only within the designated secure environment.
   3. NCTC can share, through the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI), terrorism FININTEL with U.S. Entities (per E.O. 13526 Guiding Principles for the Use of the ORCON Marking and for Sharing Classified National Intelligence with U.S. Entities).
   4. Through NCTC's Non-Title 50 VIP program, designated personnel from non-intelligence funded organizations can access ORCON FININTEL without additional permission.

H. In limited, exigent circumstances involving imminent threats to life or the U.S. Homeland, NCTC's normal policies related to data access, use, dissemination, retention,

deletion, feedback, classification and control markings, or any additional requirements may be suspended by an NCTC Deputy Director or the NCTC Chief of Staff, on a case-by-case basis.

I. Any violation of this policy may result in administrative sanction, including dismissal or return to home agency, and may be referred to ODNI authorities as appropriate for further action.

5. Roles and Responsibilities:

A. NCTC personnel will:

1. Share information in accordance with this policy. All NCTC personnel are responsible for reviewing and following requirements related to data access, use, dissemination, retention, deletion, feedback, classification and control markings, or any additional requirements.
    a. It is incumbent on NCTC personnel to seek guidance on information sharing questions rather than making individual decisions.
    b. NCTC personnel with questions related to these requirements should contact their Directorate Leadership or NCTC ISPPO for guidance.
    c. NCTC personnel will access the NCTC Data Catalog (available online on NCTC Connect), or reports generated by the Catalog, which includes specific restrictions and handling requirements for datasets and systems, when available.
2. Proactively identify and communicate to appropriate managers and to NCTC's (ISPPO) concerns about whether other agencies in the counterterrorism community are receiving sufficient access to relevant intelligence and law enforcement information.
3. Report any failure to comply with this Policy to their Directorate Leadership, as well as to NCTC Legal, and shall provide their full cooperation in any review conducted as a result of such report.

(b)(6)

Andrew M. Liepman
Principal Deputy Director
National Counterterrorism Center

19 May 2012
Date