NORTH AMERICAN AEROSPACE DEFENSE COMMAND
AND
UNITED STATES NORTHERN COMMAND

JUN 19 2009

MEMORANDUM FOR CDR NORAD and USNORTHCOM

FROM: NORAD and USNORTHCOM INSPECTOR GENERAL

SUBJECT: NORAD and USNORTHCOM J2 Procedure 15 Investigation

1. On 1 April 2008, the USMC IG, [ ], telephonically notified the N-NC/IG of a DOD 5240.1R, Activities of DOD Intelligence Components that Affect United States Persons, Procedure 15 (Procedure 15) investigation connected to a criminal investigation at Camp Pendleton that had an N&NC connection. On 18 April 2008, the FBI and NCIS provided a briefing on the criminal investigation to the Commander of NORAD and USNORTHCOM. During the brief, FBI and NCIS investigators requested that N&NC delay initiation of a Procedure 15 investigation until FBI and NCIS finished investigating the related criminal case. In anticipation of completion of the criminal investigations, the N&NC/JA, N&NC/IG, and AFOSI liaison officer (LNO) met on 23 December 2008 to determine a way ahead for initiating a N&NC Procedure 15 for activities at N&NC potentially related to the alleged criminal activities at Camp Pendleton. After consulting with the FBI and NCIS investigators on 27 January 2009, the N&NC OSI LNO informed the N-NC/IG that the criminal investigation had progressed far enough that a Procedure 15 investigation would not interfere with the criminal investigation. N-NC/IG began a Procedure 15 investigation on 13 February 2009. A timeline is provided in attachment 1. (b)(6)

2. Since late 2006, the NCIS and FBI have been investigating allegations of improper handling and compromise of national defense information. During these investigations, some information possibly indicated that two N&NC intelligence analysts [ ] passed classified material to USMC reserve personnel, and may have provided classified database checks on various subjects to these same USMC reserve personnel. (b)(6)

(b)(6) & (b)(5)

3. Based on these allegations, the focus of the N&NC Procedure 15 was to review, identify, investigate, and report any questionable N&NC intelligence activities. Specifically, the Procedure 15 focused on N&NC command processes and practices (past and present) concerning the flow of United States Persons (USPER) information, Counterintelligence (CI) information, Law Enforcement information and

other classified information into and out of the command; determine what improvements to the N&NC Intelligence Oversight Program should be made; and determine if there was possible participation of any current N-NC/J2 personnel in the release of information from N&NC related to the USMC, FBI, and NCIS investigations. Details of the Procedure 15 investigation are provided below.

a. The N-NC/IG office coordinated with the N-NC/JA office regarding the conduct of the Procedure 15 investigation, with N-NC/IG taking the lead for the investigation. The Commander, NORAD and USNORTHCOM concurred with this plan.

b. An N-NC/IG team consisting of [ ] (Deputy IG), CDR [ ] (Intelligence Inspector), working in conjunction with [ ] (NC/SJFHQ JA), began the Procedure 15 on 13 February 2009. (b)(6) & (b)(7)(C)

c. The N&NC team provided four IO training sessions to the command. The training presentation slides are attached (attachment 2). The number of J2 personnel trained reached 85% (all currently available J2 personnel were trained). The remaining personnel will receive training as soon as operationally possible.

d. The IG team conducted interviews with 24 select personnel within the J2. These interviews provided an overview of operating environments within the J2, along with potential contributing factors concerning the events leading to the alleged IO violations. The sampling body consisted of an equal number of officers, enlisted and civilian employees taken from all divisions within the J2 (J21 - J25). Several personnel who worked directly with [ ] were interviewed, as well as past supervisors and branch and division chiefs. (b)(6) & (b)(7)(C)

The interviews were conducted on [ ] from each division, ranging from SES to GG-12, and O-6 to E-5. All personnel were asked 26 questions (attachment 3) relating to: IO/USPER information and the N-NC mission, the command's IO Program, understanding of information sharing, information flow into and out of the command and overall production of intelligence within N-NC. (b)(2)

Key trends taken from responses to the questionnaire are listed below, as well as recommendations to mitigate the issue:

Issue 1: Some DOD information sharing guidelines are not understood by the majority of analysts.

Recommendation: [ ] (b)(2)(b)(5)

Issue 2: All J2 personnel need more clarity and firmer guidelines on proper receipt, use, retention, and dissemination of Law Enforcement, CI, and USPER information.

Recommendation(s):

(b)(5)(b2)

Issue 3:

(b)(5)

Recommendation:

(b)(5)
(b2)

Issue 4:

(b)(5)

Recommendation:

(b)(5)
(b2)

e. The inspection team then conducted an IO Compliance Inspection of N-NC/J2 on 5-6 Mar 2009.

(b)(5)

N-NC/J2 received an overall rating of SATISFACTORY on the inspection.

Highlights of the inspection are below:

N-NC/J2 consists of members of the U.S. Navy, U.S. Air Force, U.S. Marine Corps, U.S. Army, as well as government civilian personnel and contractors. N-NC/J2 participates in several interagency working groups and works closely with some of these organizations in

the production and dissemination of Threat Briefs, Modeling Simulations, and Intelligence Updates.

The purpose of the inspection was to ensure compliance with all Federal and DOD directives, review command IO policies, capture best practices, and discuss future IO issues in the command. The inspection team consisted of [ ], Chief of Inspections for N-NC/IG, and [ ] Intelligence Inspector for N-NC/IG. (b)(6)

[ ] N-NC/J2 Intelligence Oversight Officer (IOO), hosted the inspection team. After introductions and a presentation of objectives to [ ] the inspection began. After an initial inspection of the IO Program Continuity Book, an inspection of computer files was conducted on drives assigned to N-NC/J2. (b)(6)

This was the 5th IO Inspection conducted by the N-NC/IG.

It was clear to the inspection team that IO awareness and accountability have increased from year to year since the first inspection.

Good accountability and integration of Commercial, Law Enforcement Sensitive (LES) and other U.S. Persons information was demonstrated throughout the IO Inspection.

It was apparent that a good awareness of the legal constraints involved in IO/Sensitive Data permeated the command, and that a focused training regimen was being conducted on a frequent basis.

Attachment 4 contains the complete inspection report.

4. The N-NC/IG investigated three major areas which may have influenced or contributed to the alleged and unauthorized IO violation by [ ] (b)(6)

a. Did N-NC/J2 personnel knowingly collect information that specifically identified U.S. Persons without a foreign or CI nexus, and/or did not meet the authorized collection requirements in accordance with DoDD 5240.1-R?

The IG investigation discovered that [ ] did download prohibited information from the internet regarding U.S. Persons information and provided that information to law enforcement and other DOD elements. The IG concludes there was no evidence any other J2 personnel had knowledge of her activities, and there was no indication of others purposely committing similar violations. (b)(6)

b. Did J2 leadership influence and/or encourage the collection and/or use of improper USPER information?

No evidence of improper influence and demands was found. The N-NC/J2 leadership does encourage aggressive analysis within the rules and requires analysts to utilize multiple information sources in the production of their intelligence

products. Of 20 analysts interviewed, the majority expressed feeling pressure to produce and have all the answers, but all were adamant they were never encouraged to violate any rules or laws by N-NC/J2 leadership.

c. Is or was there a lack of understanding and, therefore, enforcement in the commands regarding the rules governing information sharing, safeguarding classified material, and collecting, utilizing, and dissemination of U.S. Persons information?

All personnel in N-NC/J2 have considerable experience in the intelligence field and all received the required annual training in IO, to include on E.O. 12333, DOD 5240.1R, and DOD 5240.1. However, the collective knowledge and understanding of the guidance contained in NNCI 14-103, E.O 12333, DoDD 5240.1, and DoDD 5240.1-R is insufficient. A large contributing factor to this confusion is the severely outdated and vague guidance provided in the DOD directives. Major issues came to light concerning the DOD directives. They do not cover the Joint operating environment well and definitions, or lack thereof, significantly lag application relative to technology advances and current threat capabilities. Application of this unclear and outdated guidance leaves room for misinterpretation, even in light of the clear objective of the commands to protect the civil liberties of US persons. Another contributing factor is the lack of clear command guidance regarding information sharing between command J2 personnel and outside analysts/agencies

5. The investigation concludes that no direct substantiation of intentional wrongdoing on the part of [ ] was found. Information to support this statement is as follows: (b)(6) & (b)(7)(c)

Issue 1: Mishandling of classified material – The sole document attributed to [ ] (b)(6) & (b)(7)(c) discovered in the course of the FBI investigation was sent through the proper email system consistent with the classification on the particular document (JWICS to JWICS). The email and attached document was sent to a coworker within the N-NC/J2 [ ] (b)(6) & (b)(7)(c) and then sent by [ ] to personnel outside the command. No mishandling of (b)(6) & (b)(7)(c) classified information by [ ] was substantiated. (b)(6) & (b)(7)(c)

Issue 2: Sharing information with Law Enforcement – Other than EO 12333 and the DOD directives, there is no clear command policy regarding the sharing of finished intelligence products with outside agencies. It became obvious through the course of the N-NC/IG Procedure 15 Investigation that appropriate and legal information sharing in the N-NC/J2 is not only accepted, it is highly encouraged by the leadership of the N-NC/J2. This is an ingrained attitude in the intelligence community (particularly since 9/11), and it was apparent that a large amount of information sharing is done on a daily basis in the command. The actions taken by [ ] of sharing [ ] area of expertise with fellow N- (b)(6) & (b)(7)(c) NC/J2 analysts were nothing out of the ordinary for an analyst in the N-NC/J2. The fact that [ ] the more senior of the two analysts, requested [ ] to provide (b)(6) & (b)(7)(c) information to [ ] was a normal function of [ ] job and was proper. No evidence (b)(6) & (b)(7)(c)

was found that showed [ ] had knowledge of [ ] improper handling (b)(6) & (b)(7)(c) of/sharing classified information with LEAs.

Recommendation: It is recommended the suspension of [ ] access to classified information be lifted and [ ] be allowed to return to work as an analyst in the J2. This is based on [ ] exemplary performance chronicled in evaluations, awards and Letters of Recommendations (spanning over 10-years), as well as unanimous positive comments from the J2 Director, [ ] Division Chief, [ ] Sr. Analyst and [ ] Branch Chief. The lack of any evidence implicating [ ] as a knowing accomplice in [ ] activities should be used to petition DIA to reinstate [ ] access to classified information. (b)(6)

6. The N-NC/IG is currently awaiting the Corrective Action Reports (CAR) on the finding from the recent IO Inspection.

7. Additionally, the N-NC/IG has addressed the propensity for similar opportunities (mishandling of USPER/Classified information) occurring in other units due to the interagency relationships and our geographic AOR. To help mitigate this, all subordinate commands have been briefed about the related risks, required sensitive information handling practices, and the multitude of channels that may carry U.S. Persons data into a command. They have been provided the appropriate references and training material.

8. POC for this report is [ ] (b)(6) & (b)(7)(c)

[ ] CAPT, USN
For WILLIAM A. MORGAN, Colonel, USAF
Inspector General

Attachments:
1. Timeline
2. IO Training Slides
3. Interview Questions
4. IO Inspection Report 09-02

cc:
ATSD (IO)
MCIG
DIA IG
N-NC J2

1st Ind, CDR N-NC

MEMORANDUM FOR THE INSPECTOR GENERAL, THE JOINT STAFF (ATTN: [redacted] (b)(4) & (b)(7)(C))

Approved/Disapproved

VICTOR E. RENUART, JR.
General, USAF

ATTACHMENT 1

N-NC J2 Proc 15 Timeline

27 Jan 09: The N-NC IO Investigator is directed by the N-NC IG to conduct a Procedure 15 in regards to the [ ] IO Issue. (b)(6) & (b)(7c)

30 Jan 09: N-NC IG IO Investigator meets with N-NC J2 Legal Advisor [( )] and IO Officer [( )]. A way-ahead was decided upon (b)(6) & (b)(7c) and initial interview questions were established.

02 Feb 09: The Joint Staff IG is officially notified of the N-NC IG intent to conduct a Procedure 15 investigation.

02 Feb 09: The N-NC PAO [( )] was informed that the Procedure 15 has (b)(6) & (b)(7c) begun to allow him to prepare a command response if needed.

09 Feb 09: N-NC IG team begins Procedure 15 Investigation of N-NC J2.

05 Mar 09: N-NC IG team conducts IO Inspection of the N-NC J2. Please see attached Inspection Report for details.

17 Mar 09: N-NC IG team completes Procedure 15 Investigation of N-NC J2. Please see attached Report of Investigation (ROI) for details.

23 Apr 09: N-NC IG receives Corrective Action Reports from N-NC J2 regarding the Finding from the 5 March IO Inspection. Please see attached Inspection Report for details.

14 May 09: N-NC JA begins IO Refresher Training for the N-NC J2. Please see attached Training Slides for details.

10 Jun 09: N-NC JA completes IO Refresher Training for the N-NC J2.

19 Jun 09: [redacted] approves Procedure 15 packet.

22 Jun 09: Completed Procedure 15 packet forwarded to JS IG and ATSD (IO)

ATTACHMENT 2

This Brief is Classified:
UNCLASSIFIED

NORAD/USNORTHCOM
Intelligence and Information Handling
Refresher Training

May-June 2009

[redacted]

N-NC/ JA and N-NC/J2JA

[redacted] (b)(6) & (b)(7c)

Purpose

- To provide refresher training on intelligence oversight and information handling
- This briefing is intended to highlight the rules and operational parameters for collection, retention, and dissemination of US person information relevant and necessary to perform the N&NC mission respective mission

Intelligence Oversight Origins

- Intelligence Oversight is a collection of policies and procedures designed to regulate and control the activity of intelligence functions and organizations
  - In response to intelligence abuses of 1960's and 70's
  - Pike & Church Committees formed to investigate Intel Community excesses:
    - Assassinations, human experimentation, domestic spying
    - FBI, CIA, military, and NSA collection against militant groups, extremists, peace groups, campus protestors

UNCLASSIFIED

Goal of Intel Oversight

- To protect the *constitutional rights* and privacy of US Persons while allowing Intelligence Components to protect the national security of the United States

- Stems from 4TH Amendment protections against unreasonable search and seizure

> ***The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall Issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. AMENDMENT IV, U.S. CONSTITUTION***

12

US Person - Definition

- Defined in under Section 101(a)(20) of the Immigration and Nationality Act

- A US Person is:
  - A United States citizen
  - A person known to be a permanent resident alien (Green Card holder)
  - Groups substantially composed of US Persons
  - Corporations Incorporated in the United States, except if directed or controlled by a foreign government

13

UNCLASSIFIED

U.S. Person Information Laws

• DOD INTELLIGENCE COMMUNITY OVERSIGHT

- *National Security Act of 1947*, Title 50, United States Code, Section 401, *et. seq.*
- *The Privacy Act*, Title 5, United States Code, Appendix 552a
- *Intelligence Reform and Terrorism Prevention Act of 2004*
- Executive Order 12333, 4 Dec 81, as amended, *United States Intelligence Activities*
- DoD Directive 5143.01, 23 Nov 05, *Under Secretary of Defense for Intelligence (USD(I))*
- DoD Directive 5148.11, 21 May 04, *Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO))*
- DoD Directive 5240.01, 27 Aug 07, *DoD Intelligence Activities*
- DoD Regulation 5240.1-R, 7 Dec 82, *Procedures Governing the Activities of DoD Intelligence Components*
- DoD Directive 5240.2, 20 Dec 07, *DoD Counterintelligence (CI)*
- DoD Instruction 5240.10, 14 May 04, *DoD Counterintelligence Support to Unified and Specified Commands*

• DOD NON-INTELLIGENCE COMMUNITY OVERSIGHT

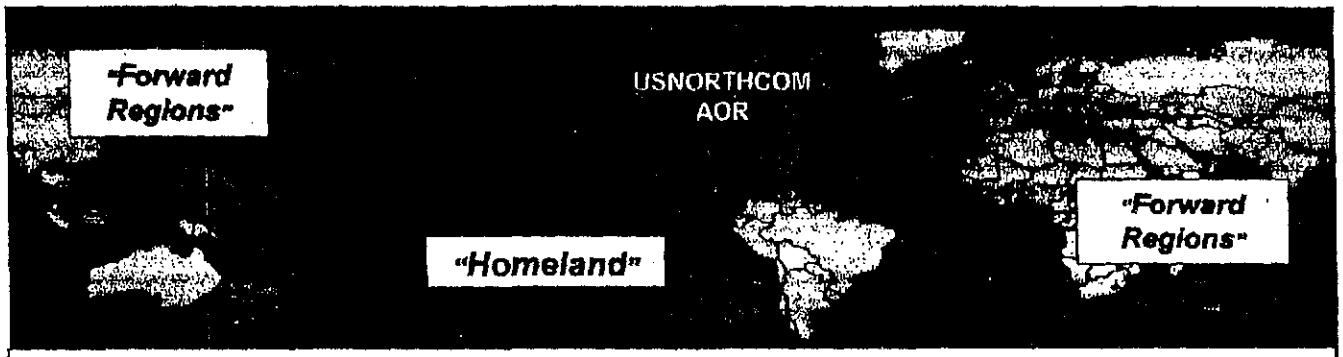
- *The Privacy Act, Title 5, United States Code, Appendix 552a*
- DoD Directive 5200.27, 7 Jan 80, *Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense*

14

UNCLASSIFIED

USNORTHCOM Mission

- Mission and AOR present unique IO challenges
  - AOR and location of ops includes U.S. homeland (285+ million US Persons)
    - The "battlefield" is within and among US Persons
    - High likelihood that some required intelligence will encompass information on US Persons
    - Force Protection occurs in the United States
  - Mission includes providing assistance to civil authorities for law enforcement and consequence management



Mission: USNORTHCOM anticipates and conducts Homeland Defense and Civil Support operations within the assigned area of responsibility to defend, protect, and secure the United State and its interests.

Balancing Interests

- USNORTHCOM ...
  - Needs information to protect DoD facilities, installations, persons, and properties, and to prevent, deny, and disrupt transnational threats
  - Needs to protect constitutional rights

- USNORTHCOM AOR and mission make this balancing of interests critical as it is subject to enhanced public scrutiny

UNCLASSIFIED

DoD IC Collecting on US Persons

Limitations on DoD Intelligence Component Mission

- National Security Act of 1947, as amended, and EO 12333, as amended, define the roles and missions of the IC.
- EO 12333 also sets intelligence oversight restrictions on collection, retention, and dissemination of information on US persons by the IC.
- DoDD 5240.01 and DoD 5240.1-R:
  - Implement EO 12333 for DoD
  - Delineateswho are the DOD intelligence components, and
  - Define what intelligence activities are authorized by those DOD intelligence components.

17

DoD IC Collecting on US Persons

Limitations on DoD Intelligence Component Mission

- The only authorized intelligence activities under the provisions of DoDD 5240.01 are foreign intelligence and counterintelligence .

18

DoD IC Collecting on US Persons

- **DoDD 5240.01 Applicable Definitions**

1 - **Intelligence Activities**: The collection, production, and dissemination of foreign intelligence and counterintelligence by DoD intelligence components authorized under [EO 12333] and [DoDD 5143.01].

2 - **Foreign Intelligence**: Information relating to the capabilities, intentions, and activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities (National Security Act of 1947).

3 - **Counterintelligence**: Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities (JP 1-02).

DoD IC Collecting on US Persons

- DoD 5240-1-R, *Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons*, implements DoDD 5240.01
- DoD 5240.1-R requires a two step test before information on US persons can be collected by a DoD IC Component:

1 - It is necessary to carry out a "function assigned" (foreign intelligence or counterintelligence + specific unit mission) the collecting component, and;

2 - It falls under one of the following categories:

- Obtained with consent
- Publicly available
- Foreign intelligence
- Counterintelligence
- Potential sources or agents
- Protection of sources or methods
- Threat to Physical security of DoD persons or installations
- Personnel security
- Communications security
- International narcotics
- To protect the safety of any person including from international terrorist organizations
- Overhead reconnaissance not targeted at specific US person/organization
- Administrative purposes

20

DoD IC Collecting on US Persons

- **EMPHASIS : Collection on US Persons allowed if there is a reason to believe the US Person is :**
  - **Connected to international terrorist activities;**
  - **Connected to international narcotics;**
  - **Connected to foreign intelligence;**
  - **A foreign or international terrorist threat to DoD installations, property, or persons; or,**
  - **The subject of authorized counterintelligence;**

- **The DoD Intelligence Component doing the collection must be conducting an assigned collection mission (foreign intelligence or counterintelligence) and follow the procedures in DoD 5240.1-R**

Collection Issues

- **Publicly Available (OSINT), Procedure 2**
  - **Must be necessary for a function assigned the collecting component – must be related to an authorized foreign intelligence (FI) or counterintelligence (CI) mission of the DoD intelligence component or person collecting the information and required by the unit's mission**

  - **If for DSCA IPB/IPE/OPB, for anticipated DSCA mission (earthquake, flooding, tornado. etc.), do you have the SecDef authority to collect for a mission other than an intelligence activity (FI or CI)?**

Collection Issues

•Classification challenges for retention of OSINT:

•Example:

• A classified CIA report (TS//HCS – trusted student source) and FBII IIR (S//NF//SI//FISA) indicate Rufus Badguy, U.S. citizen born in Minneapolis, MN, a professor of Mideast Studies at University of Texas, is part of an AQN planning cell in Austin, TX. FISA information shows direct contact with a known cell phone used by Osama Bin Laden (OBL). Translated text of cell phone conversation indicates OBL wants Rufus to recruit impressionable young US citizens for suicide attacks within the U.S. (Clear reason to believe he is connected to AQN and FI for permanent retention).

• Information available on Internet at University of Texas shows Rufus's speaking engagements at various institutions for the next 6 months (information publicly available and unclassified)

•You download the information on your NIPRNET computer. What are the rules on protecting the information from disclosure under FOIA or Privacy Act?

•You can not classify publicly available information per se – but your only basis to collect (FI or CI) is based on classified 3rd part information. You can download to NIPR, but since your authority to retain as FI is based only on classified information, your retention and use in analysis or product must be classified at the lowest level that would authorize your collection as FI In this case S/NF/FISA). So move to JWICS to retain in original form or as part of analysis and delete NIPR download

UNCLASSIFIED

Collection Issues

- **Collection Defined (DoD 5240.1-R, Procedure 2, paragraph B.1.:**
  - Collection. Information shall be considered as "collected" only when it has been received for use by an employee of a DoD intelligence component in the course of his official duties. Thus, information volunteered to a DoD intelligence component by a cooperating source would be "collected') under this procedure when an employee of such component officially accepts, in some manner, such information for use within that component. Data acquired by electronic means is 'collectedl' only when it has been processed into intelligible form.
- **Simple explanation:**
  - If you "receive" the information with an intent to use it you have collected it.
  - You can look at anything to see if can be collected, but once you make it yours (copy or store the data or file, file the e-mail for later use, incorporate the information into a product, comment on information before passing on, etc,) you have collected it under DoD 5240.1-R
  - Bits and bites in SIGINT are not in intelligible form, but raw, not finally analyzed information in written form is still considered in intelligible form
  - Information is still considered collected even if it is just a report of information collected by another agency (e.g., FBI IIR). It does not matter that the information was not directly collected by you or your component For purposes of DoD 5240.1-R applicability, information directly collected, and information received from another agency solely for analysis is treated the same -- collected.

24

Dissemination

• Dissemination (DoD 5240.1-R, Procedure 4, paragraph B.:

•Except as provided in section C., below, information about United States persons that identifies those persons may be disseminated without the consent of those persons only under the following conditions:

•1. The information was collected or retained or both under Procedures 2 and 3;

•2. The recipient is reasonably believed to have a need to receive such information for the performance of a lawful governmental function, and is one of the following:

•a. An employee of the Department of Defense, or an employee of a contractor of the Department of Defense, and has a need for such information in the course of his or her official duties;

•b. A law enforcement entity of federal, state, or local government, and the information may indicate involvement in activities which may violate laws which the recipient is responsible to enforce;

•c. An agency within the intelligence community; provided that within the intelligence community , information other than information derived from signals intelligence, may be disseminated to each appropriate agency for the purpose of allowing the recipient agency to determine whether the information is relevant to its responsibilities without such a determination being required of the disseminating DoD intelligence component;

•d. An agency of the federal government authorized to receive such information in the performance of a lawful governmental function; or

•e. A foreign government, and dissemination is undertaken pursuant to an agreement or other understanding with such government.

25

Unauthorized Disclosure of Classified

- **18 USC 798. Disclosure of classified information:**

  - **(a) Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States any classified information—**

    - **(1) concerning the nature, preparation, or use of any code, cipher, or cryptographic system of the United States or any foreign government; or**

    - **(2) concerning the design, construction, use, maintenance, or repair of any device, apparatus, or appliance used or prepared or planned for use by the United States or any foreign government for cryptographic or communication intelligence purposes; or**

    - **(3) concerning the communication intelligence activities of the United States or any foreign government; or**

    - **(4) obtained by the processes of communication intelligence from the communications of any foreign government, knowing the same to have been obtained by such processes—**

- **Shall be fined under this title or imprisoned not more than ten years, or both.**

Unauthorized Disclosure of Classified

18 USC § 1924. Unauthorized removal and retention of classified documents or material:

- (a) Whoever, being an officer, employee, contractor, or consultant of the United States, and, by virtue of his office, employment, position, or contract, becomes possessed of documents or materials containing classified information of the United States, knowingly removes such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location

- shall be fined under this title or imprisoned for not more than one year, or both.

27

Unauthorized Disclosure of Classified

50 USC 783. Offenses

• (a) Communication of classified information by Government officer or employee : It shall be unlawful for any officer or employee of the United States or of any department or agency thereof, or of any corporation the stock of which is owned in whole or in major part by the United States or any department or agency thereof, to communicate in any manner or by any means, to any other person whom such officer or employee knows or has reason to believe to be an agent or representative of any foreign government, any information of a kind which shall have been classified by the President (or by the head of any such department, agency, or corporation with the approval of the President) as affecting the security of the United States, knowing or having reason to know that such information has been so classified, unless such officer or employee shall have been specifically authorized by the President, or by the head of the department, agency, or corporation by which this officer or employee is employed, to make such disclosure of such information.

•(c) Penalties for violation : Any person who violates any provision of this section shall, upon conviction thereof, be punished by a fine of not more than $10,000, or imprisonment for not more than ten years, or by both such fine and such imprisonment, and shall, moreover, be thereafter ineligible to hold any office, or place of honor, profit, or trust created by the Constitution or laws of the United States.

•(e) Forfeiture of property : (1) Any person convicted of a violation of this section shall forfeit to the United States irrespective of any provision of State law—

•(A) any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation; and

•(B) any of the person's property used, or intended to be used, in any manner or part, to commit, or to facilitate the commission of, such violation.

28

Unauthorized Disclosure of Classified

Administrative Penalties

- Loss of Security Clearance
- Loss of Employment
- Other Administrative Actions as authorized under civilian personnel law

Use of DoD IC Components Capabilities for Other Than "Intelligence Activities"

- **DoD IC Component Authorities/Limitations**
  - **The Secretary of Defense may use ANY assets of DoD to accomplish a valid DoD mission**
    - **Use of DoD IC Component Capabilities for other than "intelligence activities" (FI or CI) requires approval of both the mission and the specific use of the DoD IC component capability by the Secretary of Defense**
    - **RFA/RFF process requesting the specific capabilities of the DoD IC component will be submitted through JOPES for review and approval by JS and SECDEF, with recommendations on any limitations on use of the DoD IC component capabilities or data collected or products derived therefrom**
    - **SECDEF approved EXORD authorizing use of the DoD IC component capabilities and setting forth any operational parameters or limitations is required**
  - **Types of DoD IC component capability support for other than intelligence activities**
    - **Defense Support of Civil Authorities (DSCA) – (hurricane disaster support, wildfires, etc. – incident awareness and assessment (IAA), search and rescue (SAR), damage assessment)**

30

Use of DoD IC Components Capabilities for Other Than "Intelligence Activities"

- **DoD Intelligence Component Capabilities**

  - **People**
    - **–Military or civilian personnel employed in an Intel capacity, e.g. Intel analysts, J2 personnel**
  - **Equipment**
    - **–Paid for with Intelligence funding, e.g.**
      - **–UAS (Predator)**
      - **–Intelligence communications - website portals, imagery software, data processing**
  - **Capabilities**
    - **–Sources of raw data, e.g. SIGINT, IMINT, MASINT**
    - **–Products, e.g. finished reports and studies**
    - **–ISR activities**
    - **–Processes, e.g., research, tasking, analysis, dissemination**

Use of DoD IC Components Capabilities for Other Than "Intelligence Activities"

- **Are we using a DoD intelligence component capability?**
  - **QUESTIONS TO ASK:**
    - **Do we have the proper authority?**
    - **What is the big picture mission?**
    - **What exactly will be done?**
    - **Who will be doing it?**
    - **What equipment will be used to do it?**
    - **Where will it be done?**
    - **Who or what is being targeted?**
    - **Are we collecting information or data?**
    - **How will it be collected?**
    - **How will it be processed and disseminated?**
    - **Does it require a security/classification review?**

32

UNCLASSIFIED

Use of DoD IC Components Capabilities for Other Than "Intelligence Activities"

- **Types of DoD IC component capability support for other than intelligence activities**

  - **Defense Support to Civil Authorities (DSCA)** – (hurricane disaster support, wildfires, etc. – incident awareness and assessment (IAA), search and rescue (SAR), damage assessment)

  - **Computer Network Defense Response actions (CND-RA)** – requires SecDef approval to use DoD IC capabilities to provide support for other than FI or CI

  - **Military Support to Civilian Law Enforcement (MSCLEA)** – Must follow procedures in DoDD 5525.5, and must be approved by SecDef
    - **Example: DC Sniper Support to FBI**
    - **Note: International Counter Drug (CD) support would normally be an "intelligence activity" support to LEA (FI) processed under DoD 5240.1-R, Procedure 12 and DoDD 5525.5**

2008 CJCS Standing DSCA EXORD

- Provides SecDef authorization to use traditional Intelligence capabilities to conduct DSCA missions for non-intelligence purposes
- Designates IAA packages as part of Tier 3 forces
- Sourced through ISR Response Force on PTDO status
- IAA may be used for:
  - Situational Awareness
  - Damage Assessment
  - Evacuation Monitoring
  - SAR
  - CBRNE Assessment
- Requires a validated mission assignment (MA) from Primary Agency before authority exists
- Does not authorize imagery collection for IPB/IPE/OPE in advance of actual disaster and MA to assist operational planning for "anticipated" DSCA mission
- Intelligence Oversight Rules apply.

34

Legal and Policy Considerations

- Authorities, Allocations, and Proper Use

  - Authorities:

    - Statutory, UCP, EXORDS

    - Service Requirements

  - Allocations:

    - Global force Management Allocations (GFM) by FY

    - Command Owned

  - Proper Use:

    - Training – Approved through Service channels – no authority for retention of imagery for operational use past the training requirement. To use for operational purposes after training, JS/OSD approval is required

    - Operational - Review for proper use must consider further dissemination of products by unintended. If conducted pursuant to CJCS DSCA EXORD, as for modification to intelligence/information collection restrictions

35

Legal and Policy Considerations

- **Dissemination**

  - **Airborne Sensors - DoDI 5210.52, Security Classification of Airborne Sensor Imagery and Airborne Imaging Systems, DIAI 5210.001, Security Classification of Airborne Sensor Imagery, requires declassification review of all data from airborne sensors before dissemination – who performs this function? N-NC for N-NC missions, unless delegated**

  - **NTM and Overhead under NGA control – DoDI 5210.52 and NGA regulations and policy control at**
    - http://policy.nga.smil.mil/policy_guidance/ips/gipsips/gipsips_secret.cfm

- **Review of Domestic Imagery Requests for Proper Use**

  - **N-NC requires components forward requests for domestic imagery to N-NC for review of proper use (N-NC J2 OI 14-3)**

    - **NTM and Overhead - NGA requires a Proper Use Memorandum (PUM) with a specific format be forwarded for approval for all NGA controlled assets when requesting domestic imagery – 1 approval for recurring requirement see**
      http://policy.nga.smil.mil/policy_guidance/ips/gipsips/ips8b.pdf

    - **DIA MSG 232805Z NOV 01, SUBJ: New Procedures for the Approval of DoD Domestic Airborne Reconnaissance Imagery Proper Use Statements (U) – Commands may approve, but recommends formalization of review process for proper use. New procedures not effective until processes forwarded to DIA and approved.**

36

ISR/IAA Factors Affecting Legal and Policy Issues

- **Specific Platform Capabilities**
  - **Data Feed**
    - **How is the data transmitted? – satellite bounce to remote location, wet film, direct feed, ROVER relay, sample analysis processed at remote site and transmitted by mail, electrons, etc.**
    - **Who is or will be the ultimate consumer? – What is the classification level of the sensor or metadata collected, can it be declassified, does it reveal source and methods**
    - **How does the sensor operate? – fixed or turnable lens; extended loiter capability; ground, air breather, or NTM overhead**
  - **Ownership/Control of Sensor**
    - **Service controlled or deployed in support of N-NC mission?**
    - **Who is the security/declassification authority under DoDI 5210.52 and DIAI 5210.001?**

N-NC I 14-103, Intelligence Oversight

- Published 17 April 2007, located on command portal at
- https://operations.noradnorthcom.mil/sites/CommandGroup/ChiefOfStaff/pubsandforms/default.aspx

•Applicable to all Intelligence components and personnel of NORAD and USNORTHCOM and its components

•Requires marking of U.S. Person information in all products produced by NORAD or USNORTHCOM intelligence components

•Provides guidance on use of DoD intelligence component capabilities for missions other than FI or CI

• Provides factors to consider to help frame analyst's "reason to believe a US Person is involved in foreign intelligence (FI) or counterintelligence (CI)

38

N-NC I 14-3, Domestic Imagery

- **Published 5 May 2009, located on command portal at**
- **https://operations.noradnorthcom.mil/sites/CommandGroup/ChiefOfStaff/pubsandforms/default.aspx**

•Applicable to all intelligence components and personnel of NORAD and USNORTHCOM and its components

•Applies to all domestic imagery – NTM, airborne, surface, maritime surface and maritime sub surface.

•Provides consolidated guidance on process and format for requesting and reviewing requests for domestic imagery.

UNCLASSIFIED

Intelligence Oversight Reporting and Enforcement

- **The Assistant to the Secretary of Defense for Intelligence Oversight**
  - Responsible for oversight of all DoD intelligence activities
  - Promulgates guidance for inspecting intelligence activities for intelligence oversight compliance
  - DoD Policy – Intelligence Oversight Reporting Criteria, 17 July 2008
- **Inspector Generals**
  - Responsible for inspections of intelligence components
  - Receive reports of and investigate questionable intelligence activities
- **General Counsels (Staff Judge Advocate)**
  - Responsible for receiving reports of questionable intelligence activities
  - Providing legal guidance to intelligence components regarding collection, retention and dissemination of US person information

40

Questions

QUESTIONS?

NORAD-USNORTHCOM J2JA

[redacted] (b)(6)

NORAD-USNORTHCOM JA

[redacted] (b)(6)

NORAD USNORTHCOM JA Office

(719) 554-9193

41


NORTH AMERICAN AEROSPACE DEFENSE COMMAND


UNITED STATES
NORTHERN COMMAND

ATTACHMENT 3

Interview Questions for N-NC J2 Personnel

Name:_____ **Date:**_____

1. [redacted] (b)(2)

2. [redacted] (b)(2)

3. [redacted] (b)(2)

4. [redacted] (b)(2)

5. [redacted] (b)(2)

6. [redacted] (b)(2)

7. [redacted] (b)(2)

8. [redacted] (b)(2)

9. [redacted] (b)(2)

10. [redacted] (b)(2)

11. [redacted] (b)(2)

12. [redacted] (b)(2)

13. [redacted] (b)(2)

14. [redacted] (b)(2)

15. [redacted] (b)(2)

16. [redacted] (b)(2)

17. [redacted] (b)(2)

18. [redacted] (b)(2)

19. [redacted] (b)(2)

20. [redacted] (b)(2)

21. [redacted] (b)(2)

22. [redacted] (b)(2)

23. [redacted] (b)(2)

24. [redacted] (b)(2)

25. [redacted] (b)(2)

26. [redacted] (b)(2)

ATTACHMENT 4

For Official Use Only

UNITED STATES NORTHERN COMMAND

OFFICE OF THE INSPECTOR GENERAL

[redacted]

IO Inspection 09 – 02a

NORAD-USNORTHCOM J2

Peterson AFB, CO

05 March 2009

TABLE OF CONTENTS

SECTION I – Visit Summary

General: The N-NC IG conducted an Intelligence Oversight Inspection of the N-NC J2, Peterson Air Force Base, CO, on 5 March 2009. The J2 consists of members of the U.S. Navy, U.S. Air Force, U.S. Marine Corps, U.S. Army, as well as government civilian personnel and contractors. The N-NC J2 participates in several Interagency Working Groups and works closely with some of these organizations in the production and dissemination of Threat Briefs, Modeling Simulations, and Intelligence Updates.

The purpose of the visit was to ensure compliance with all Federal and DOD directives, review command IO policies, capture best practices. and discuss future IO issues in the command. The inspection team consisted of [redacted] Chief of Inspections, for N-NC IG, and [redacted] Intelligence Inspector for N-NC IG. (b)(6) & (b)(7c)

[redacted] N-NC J2 Intelligence Oversight Officer (IOO), hosted the inspection team (b)(6) & (b)(7c) After introductions and a presentation of objectives to [redacted] the inspection began (b)(6) & (b)(7c) Following an initial inspection of the IO Program Continuity Book, an inspection of computer files was conducted on drives assigned to the J2 shop.

This was the 5th IO Inspection conducted by the N-NC IG and it was clear to the inspection team that IO awareness and accountability have increased from year to year since the first inspection. Good accountability and integration of Commercial, Law Enforcement Sensitive (LES) and other U.S. Persons information was demonstrated throughout the IO Inspection. It was apparent a good awareness of the legal constraints involved in IO/Sensitive Data permeated the command, and that a desire to protect the civil liberties of individuals was endorsed from the top down.

References used during the inspection:

a. EO 12333, US Intelligence Activities
b. DoD 5240.1-R, Procedures Governing Activities of DoD Intel Components that Affect US Persons
c. DoDD 5240.01, DoD Intelligence Activities
d. CJCSI 5902.01, Oversight of Intelligence Activities
e. N-NC Instruction 14-103, Intelligence Oversight
f. NORAD Instruction 90-203, Inspector General Activities

SO

SECTION II – Inspection System

1. **Rating System:**

SATISFACTORY	Performance or operation meets mission requirements. Procedures and activities are carried out in an effective and competent manner. Resources and programs are adequately managed. Deficiencies exist, but do not significantly limit mission accomplishment.
UNSATISFACTORY	Performance or operation does not meet mission requirements. Procedures and activities are not carried out in an adequate manner. Resources and programs are not adequately managed. Significant deficiencies exist that preclude or seriously limit mission accomplishment.

2. Report-Writing System:

FINDINGS	Those areas where the inspected organization does not comply with an identifiable standard constitutes a finding. The organization is required to take corrective action and provide a written response to the COCOM IG. Findings are core problems that need to be reviewed by the NORAD and USNORTHCOM staff and are indicated by an asterisked alphanumeric symbol in parentheses *(RFY-01). Any critical or major deficiency resulting in an "Unsatisfactory" rating may result in a finding. Findings are sequentially numbered for each U.S. fiscal year. The rated unit, unless there is another designated OPR for the finding, must answer these findings. Refer to Section IV, paragraph 3, for the proper handling of Finding replies.
OBSERVATIONS	An observation is an opinion where a standard may not have been violated or may not exist, but where economy, efficiency, or effectiveness may be improved by recommended corrective actions.
NOTABLES	Those areas where an organization is operating in an excellent manner. Unlike commendables, notables are not forwarded or exported.
COMMENDABLES	Those areas where an organization is operating in an outstanding manner. Commendables are "best practices" or procedures that can be exported to other organizations. The NORAD and USNORTHCOM IG maintains a database of Commendables which is accessible on its portal page: https://operations.noradnorthcom.mil/sites/CommandSpecialStaff/IG/USNORTHCOMIG/default.aspx.

SECTION III – Inspection Summary

1. **Inspection Results:**

OVERALL RATING	**SATISFACTORY**
PROGRAM BOOK	**SATISFACTORY**
IO Pubs/Directives	SATISFACTORY
Training Records	SATISFACTORY
Appointment Orders	SATISFACTORY
TRAINING PROGRAM	**UNSATISFACTORY**
SELF-INSPECTION	**UNSATISFACTORY**
JA INVOLVEMENT	**SATISFACTORY**
QUARTERLY REPORTING	**SATISFACTORY**
FINDINGS	**NONE**
OBSERVATIONS	**FOUR**
NOTABLES	**THREE**
COMMENDABLES	**TWO**

2. **General:** The N-NC Inspector General conducted an Intelligence Oversight (IO) inspection of the N-NC J2 at Peterson AFB, CO on 5 March 2009.

3. **Participants:** All elements of the J2 were inspected. Due to the large size of the J2 Directorate.

(b)(2)

SECTION IV – Narrative

1. Program Book – Satisfactory

1.1. IO Pubs/Directives - Satisfactory

NOTABLE

- The development of a very inclusive, detailed, and user friendly IO Program Book greatly facilitates the overall running of the program. Not only does the book contain all required items, it also contains a large amount of additional IO related white-papers, point papers, and other items of interest. In addition, the updated local N-NC J2 OI helps to ensure the standardization of daily operating procedures and activities. This standardization will help prevent a possible IO violation or incident.

1.2. Training Records – Satisfactory

NOTABLE

- The Training Records section of the Program book was detailed and complete. The spreadsheet made it very easy to track individual training by section, as well as completion/due date.

1.3. Appointment Orders – Satisfactory

NOTABLE

- Numerous flyers that denote the Intelligence Oversight Officer (IOO) for the command were readily visible in conspicuous places throughout the area. These flyers enhance the availability of the IO Officer to personnel within the unit.

2. Training Program – Unsatisfactory

OBSERVATION

- With the exception of the IOO and the assistant IOO, ~~only one person out of 26 polled had ever read the N-NCI 14-103 (IO Instruction), and only a few more had even heard of it.~~ The lack of familiarity with the N-NC IO Instruction shows a systemic problem with the IO training currently conducted.

3. Self Inspection – Unsatisfactory

OBSERVATIONS

- There was evidence the efficiency and depth of the self inspections conducted were not as detailed as they could be. A search of databases resulted in finding one document stored on a hard drive that contained questionable historical data that included USPER information. The document dated back to 2006, and no evidence of it being used was found. A determination was made by the N-NC IG and the N-NC J2 legal advisor [redacted] that due to the type and limited quantity of information (one DHS report), and the fact that the document had not been utilized in any intelligence products, no violation had occurred. (b)(6)

[redacted] This should result in a manageable volume being reviewed periodically. Documentation of the self inspection, to include date, areas inspected (files, drives, etc.) and actions taken if any, should be maintained. Several other self inspection techniques were discussed, as well as various types of incoming material that should be screened closely for possible IO violations (Law Enforcement Products, CI Products, etc). (b)(2)

- The shared drive for the J2 is extremely cluttered. There were numerous files/documents saved multiple times in different locations, and many instances of multiple versions of the same document being maintained on the drive. Many of these documents were PowerPoint briefings containing imagery taking up large amounts of disk space. The main concern that the IG team had with the duplication of data is the extra clutter located on the shared drive hindering an effective self inspection program.

4. JA Review and Collaboration – Satisfactory

COMMENT

- The IG team noted during the inspection the N-NC J2 legal advisor does not have access to all J2 documents, but the IOO does. To ensure good IO review, the IOO must ensure he collaborates with the N-NC J2 legal advisor on all questionable items.

5. Quarterly Reporting – Satisfactory

- The content of the reports provide insight and information to meet the requirement.

SECTION V – Associated Inspection Items

1. **Commendables –**

   - A recently adopted method of tracking all USPER information/holdings developed by the J21 is excellent. The inclusive spreadsheet will simplify the periodic review/validation of current holdings, and provide an easy means of tracking the deletion of this information.

   - Superb IO signage is located throughout all Divisions and Branches within the J2. These detailed posters provide the analysts with a flowchart walking them though the "Foreign Nexus" determination matrix. Not only do they provide detailed guidance on proper collectability and retention of USPER info, they deliver a constant reminder of IO requirements.

2. **Findings – One**

   - ***(R09-01)**

     Finding Statement: **Un-redacted USPER data archived on J2 drives**

     Standard: **E.O 12333, DoDD 5240.1, DoD 5240.1-R, NNCI 14-103.**

     Office of Primary Responsibility: **N-NC J2, J6, SJA**

     Discussion: [

     (b)(2)

     ]

     Recommended Actions(s): **This is a policy issue and not done by any individual analysts. The N-NC legal advisor is currently working with the N-NC SJA office on a Legal Decision Paper to support the J2 doing this. Additionally, a legal reading should be sought from DoD General Counsel to ensure compliance with DoD guidelines.**

3. **Finding Reply Instructions:** If this report contains a Finding, it is answerable to the NORAD-USNORTHCOM/IG not later than 30-days after receipt of the Inspection report.

3.1. Corrective Action Reports will be in the following format:

IO R06-01 (and the finding statement) followed by the corrective action being taken. The finding statement will be extracted from the Inspection report and typed in **BOLD CAPITAL** letters. Replies should provide sufficient detail to permit OPR and IG to determine whether or not to close the finding.

3.2. Corrective Action Report Extensions: When corrective actions cannot be completed by the time of reply date, describe the action proposed or in progress and state the estimated completion date (Open: ECD Day/Month/Year). If the action is beyond the capability of the unit, describe the action being taken to obtain assistance.

3.3. Forward corrective action reports to the following address, with an information copy, if applicable, to the parent unit.

HQ NORAD-USNORTHCOM / IG
250 Vandenberg St Ste B016
Peterson AFB, CO 80914-3800

3.4. The NORAD-NORTHCOM IG will staff the corrective action report with appropriate staff agencies.

4. POC for action is [redacted] (b)(6) & (b)(7c)

////////////////ORIGINAL SIGNED////////////////
WILLIAM A. MORGAN, Colonel, USAF
NORAD-USNORTHCOM IG

cc:
1. N-NC J2
2. N-NC J2 Legal Advisor
3. N-NC IOO

NORTH AMERICAN AEROSPACE DEFENSE COMMAND
AND
UNITED STATES NORTHERN COMMAND

20 Apr 2009

MEMORANDUM FOR NORAD-USNORTHCOM Inspector General

FROM: N-NC J2 Intelligence Oversight Officer

SUBJECT: CORRECTIVE ACTION REPORT FOR NORAD/USNORTHCOM IG Intelligence Oversight (IO) Inspection, 5 Mar 2009

1. NORAD/USNORTHCOM IG Inspection Team conducted an IO inspection on 5 Mar 2009. Below is their one finding accompanied by the corrective action.

IO R09-01: UN-REDACTED USPER DATA ARCHIVED ON J2 DRIVES

CORRECTIVE ACTION: Per the IG's recommendation, the N-NC J2 Operations Law attorney is working with the N-NC Staff Judge Advocate office on a Legal Decision Paper to support the archival. He is also seeking a legal reading from the DoD General Counsel to ensure compliance with DoD guidelines. This action was approved by [redacted] (N-NC/J2) on 7 Apr 09. (b)(6) & (b)(7c)

2. As recently as 16 April 2009, the N-NC/J2JA received an [redacted]

(b)(2)

3. Questions concerning this response can be addressed to [redacted] 5. (b)(6) & (b)(7c)

//SIGNED//
[redacted], Lt Col, USAF (b)(6) & (b)(7c)