DEPARTMENT OF THE ARMY
U.S. ARMY COMBINED ARMS CENTER AND FORT LEAVENWORTH
415 SHERMAN AVENUE UNIT 2
FORT LEAVENWORTH, KANSAS 66027-2300

REPLY TO
ATTENTION OF:

ATZL-CG

14 February 2011

MEMORANDUM FOR Secretary of the Army

SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

1. (U//~~FOUO~~) On 16 December 2010, I was appointed to conduct an AR 15-6 Investigation into the Compromise of Classified Information to Wikileaks. This report is the result of a comprehensive, multi-disciplinary, and independent administrative investigation into the facts and circumstances associated with the suspected compromise of classified national security information by Private First Class (PFC) Bradley E. Manning to the Wikileaks organization. Facts related to PFC Manning's alleged criminal misconduct are being investigated by law enforcement agencies and the ultimate disposition will be in accordance with prescribed laws and regulations. Findings and recommendations concerning PFC Manning's alleged criminal misconduct are outside the scope of this investigation. Nothing contained herein should be viewed as an expression of his guilt or innocence.

2. (U//~~FOUO~~) No Adverse Impact Due to Witness or Information Unavailability. Every effort was made to review all available materials, regulations and policies relating to the investigation. The investigative team was able to conduct interviews of all necessary and relevant witnesses with three exceptions (PFC Manning's aunt, one of his close friends, and PFC Manning himself). In accordance with the direction in the appointment memorandum not to interfere with the ongoing criminal investigation, PFC Manning's aunt and close friend were unavailable for interview. PFC Manning was not approached due to his initial Article 31 rights invocation on 8 May 10 and his attorney's 23 July 2010 email to the United States Forces-Iraq (USF-I) 15-6 Investigating Officer indicating that "because PFC Manning faces serious charges which have already been preferred, we are not inclined to make him available for an interview." (DA Form 3881, PFC Manning, 8 May 10 (Encl N6) and USF-I 15-6, Pages 30-31, 26 Jul 10 (Encl R1)). Subsequent thereto, PFC Manning retained civilian counsel, in addition to his detailed military counsel. Considering the charges pending against PFC Manning, his earlier rights invocation, and his counsel's stated rationale not to allow an interview in an earlier 15-6 investigation, the investigative team had no reason to believe that PFC Manning would cooperate with this investigation.

3. (U//~~FOUO~~) It is my opinion that this investigation was not adversely impacted by the unavailability of these three witnesses. Enclosure D contains a full documentation of the appointing official's instructions and my investigative methodology.

4. (U//~~FOUO~~) Report Organization. This report is separated into five discrete sections.

a. (U//~~FOUO~~) Section I: Facts and Background Information Pertaining to PFC Manning and the 2d Brigade Combat Team (BCT), 10th Mountain Division (2/10 MTN). Section I is further divided into five sections.

(1) (U//~~FOUO~~) Section IA: PFC Manning.

(2) (U//~~FOUO~~) Section IB: Chain of Command.

(3) (U//~~FOUO~~) Section IC: Personnel Security (Security Clearances).

(4) (U//~~FOUO~~) Section ID: Sensitive Compartmented Information (SCI) Physical Security.

(5) (U//~~FOUO~~) Section IE: Behavioral Health.

b. (U//~~FOUO~~) Section II: Regulations, Policies and Facts Pertaining to Information Assurance.

c. (U//~~FOUO~~) Section III: Leading the New Generation and Understanding Its Culture.

d. (U//~~FOUO~~) Section IV: Findings and Recommendations Relating to Information Assurance, Personnel Security, Physical Security and Behavioral Health. Section IV is further divided into 4 sections.

(1) (U//~~FOUO~~) Section IVA: Findings and Recommendations Pertaining to Information Assurance.

(2) (U//~~FOUO~~) Section IVB: Findings and Recommendations Pertaining to Personnel Security.

(3) (U//~~FOUO~~) Section IVC: Findings and Recommendations Pertaining to SCI Physical Security.

(4) (U//~~FOUO~~) Section IVD: Findings and Recommendations Pertaining to Behavioral Health.

e. (U//~~FOUO~~) Section V: Individual Responsibility.

f. (U//~~FOUO~~) Section VI: Appendices.

(1) (U//~~FOUO~~) Appendix 1: Personnel Listing.

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

(2) (U//~~FOUO~~) Appendix 2: Investigative Team Members.

(3) (U//~~FOUO~~) Appendix 3: Abbreviations/Acronyms.

(4) (U//~~FOUO~~) Appendix 4: Abbreviations of Ranks.

(5) (U//~~FOUO~~) Appendix 5: Definitions.

(6) (U//~~FOUO~~) Appendix 6: References.

(7) (U//~~FOUO~~) Appendix 7: Detailed Exhibit Listing.

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

Table of Contents (U)

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

SECTION I:
Facts and Background Information Pertaining to PFC Manning and the 2d Brigade Combat Team (BCT), 10th Mountain Division (2/10 MTN).

Section IA: PFC Manning

1. (U//~~FOUO~~) Before Joining the Army.

a. (U//~~FOUO~~) Birth through High School Graduation. Bradley Edward Manning was born on [redacted], in Oklahoma City, Oklahoma. (Enlisted Record Brief (ERB), 2 May 2010 (Encl J)). He remained in Oklahoma with his parents, [redacted] (later [redacted]) and [redacted], until they divorced in 2001. In November 2001, PFC Manning[1] departed the United States (U.S.) to live with his mother in Wales, United Kingdom (UK) - her country of citizenship. (Standard Form (SF) 86/Investigator Notes, SF 86, 6 Dec 07 - 7 Dec 07 (Encl N1)). PFC Manning graduated high school on 9 June 2005 and returned to the United States in September 2005. (SF 86/Investigator Notes, 6 Dec 07 - 7 Dec 07 (Encl N1)).

b. (U//~~FOUO~~) PFC Manning's Return to the U.S.

(1) (U//~~FOUO~~) [redacted] Upon his return to the U.S., PFC Manning lived with his father and stepmother in Oklahoma City. (SF 86 Application/Investigator Notes, 6 Dec 07 - 7 Dec 07 (Encl N1)). There was conflict between PFC Manning and his stepmother. In December 2009, PFC Manning reported to a military behavioral health provider that in 2005 his father had taken him to a family doctor due [redacted]. At that time, PFC Manning was [redacted] PFC Manning's records indicate [redacted] (Behavioral Health Records, 25 Dec 09 (Encl M1-1)). As discussed later, in section IC, PFC Manning failed to disclose, at time of enlistment or on his SF 86, the fact that he saw a medical professional for behavioral health issues. (SF 86/Investigator Notes, 6 Dec 07 - 7 Dec 07 (Encl N1)).

(2) (U//~~FOUO~~) Conflict with Stepmother. According to PFC Manning, he lived with his father and stepmother until 10 April 2006, when his stepmother called the Oklahoma City Police Department and reported that PFC Manning threatened her and that she wanted him to move out of the house. PFC Manning stated he did not know

[1] (U) Throughout this report, Bradley Edward Manning will be referred to as PFC Manning to reflect his current rank and to avoid any confusion. Where his rank is a material fact, the report will indicate his rank at the time referenced.

why his stepmother had called the police, and no official action was taken after he spoke with the police and agreed to leave the house. (SF 86/Investigator Notes, 6 Dec 07 - 7 Dec 07 (Encl N1)). A National Crime Information Center (NCIC) database search on Bradley E. Manning, conducted as part of his security clearance investigation, failed to reveal any adverse criminal information, to include any mention of the alleged threat made towards his stepmother. (Advance Fingerprint Report, 26 Oct 07 (Encl O5)).

c. (U//~~FOUO~~) April 2006 to October 2007.

(1) (U//~~FOUO~~) For Your Entertainment (FYE) Employment. After PFC Manning moved out of his father's home, he began working at FYE, in Tulsa, OK. He was employed at FYE as an Assistant Manager from 10 April 2006 through 9 June 2006, only 61 days. (SF 86, Investigator Notes, 6 Dec 07 - 7 Dec 07 (Encl N1)). PFC Manning was fired from FYE for failing to meet sales goals. (SF 86/Investigator Notes, 6 Dec 07 - 7 Dec 07 (Encl N1)). When asked on the SF 86, Block 20 whether he was ever "fired" from a job, he responded "NO." (SF 86 Application, 26 Sep 07 (Encl N3)). The SF 86 discrepancy is discussed in section IC.

(2) (U//~~FOUO~~) Coopermill Apartments, Tulsa, OK. PFC Manning moved into the Coopermill Apartments on 18 April 2006. Records at the apartment complex indicate that he was the only person living in the apartment. He paid the May rent on time, but was late paying the June rent. On 12 July 2006, the bookkeeper discovered the apartment empty with keys on the counter. PFC Manning's exact date of departure is unknown since he "skipped out" on the lease. PFC Manning owed Coopermill Apartment $1,472.51 for past rent, cleaning, damages, and termination fee. (SF 86, Investigator Notes, 18 Dec 07 - 27 Dec 07 (Encl N1)). PFC Manning failed to disclose the debt on his security clearance form. (SF 86 Application, 26 Sep 07 (Encl N3)).

(3) (U//~~FOUO~~) PFC Manning's Move to Maryland. In July 2006, PFC Manning moved to Maryland to live with his aunt, (b) (6), (b) (7)(C) [redacted]. PFC Manning lived with his aunt until he joined the Army in October 2007. During this period of time, PFC Manning took classes at Montgomery College and worked at Starbucks. (SF 86/Investigator Notes, 18 Dec 07 - 27 Dec 07 (Encl N1)). While PFC Manning lived with his aunt, she took him to a physician because he was (b) (6), (b) (7)(C) [redacted]. PFC Manning was (b) (6), (b) (7)(C) [redacted]. Again, PFC Manning reported that he [redacted] (Behavioral Health Records, 24 Dec 09 (Encl M1-1)).

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

2. (U//~~FOUO~~) Accession into the Army.

a. (U//~~FOUO~~) As part of PFC Manning's accession into the Army, he reported to the Fort Meade Military Entrance Processing Station (MEPS) on or about 31 August 2007. The MEPS processing includes a medical examination which is documented on a DD Form 2807-1 (Encl O23), Report of Medical History. The form includes a series of questions covering behavioral health issues. (b) (6), (b) (7)(C) [redacted]

b. (U//~~FOUO~~) The enlistment criteria are set out in AR 601-210, Active and Reserve Components Enlistment Program, 7 June 2007 and AR 40-501, Standards of Medical Fitness, 29 May 2007. Paragraph (b) (6), of AR 40-501 lists the criteria for which (b) (6), (b) (7)(C) would disqualify an individual from military service. Specifically, it states (b) (6), (b) (7)(C) [redacted] AR 40-501, paragraph (b) (6), 29 May 2007 (Encl Q54)).

c. (U//~~FOUO~~) Despite the behavioral health issues identified in paragraphs 1.b.(1). and 1.c.(3). above, PFC Manning answered (b) (6), (b) (7) in the negative. There is no other indication of behavioral health review or screening in PFC Manning's enlistment documents. (PFC Manning's DD Form 2807-1, Report of Medical History, 31 August 2007 (Encl J1)).

d. (U//~~FOUO~~) On 26 September 2007, PFC Manning began his four year enlistment in the Active Army. (Enlistment Docs (Encl J1)).

3. (U//~~FOUO~~) MOS Classification. PFC Manning's enlistment was for service as a Military Occupational Specialty (MOS) 35F, Intelligence Analyst. (See DA Form 3286 (Annex A), dated 26 Sep 2007, U.S. Army Delayed Enlistment Program (Encl J1); DA Form 3286 (Annex B), dated 2 Oct 2007, United States Army Enlistment Program (Encl J1)). In order to be granted the MOS of 35F, PFC Manning needed to meet the requirements set out in Department of the Army (DA) Pam 611-21. The requirements included: a score of 101 or higher on the ST (skilled technical) portion of the Armed Services Vocational Aptitude Battery (ASVAB); eligibility for a Top Secret/Sensitive Compartmented Information (TS/SCI) security clearance; a high school or equivalent degree; no criminal conviction for anything other than minor traffic violations; U.S. citizenship; and the absence of any no close ties to foreign countries within whose boundaries physical or mental coercion is known to be common. PFC Manning met all the requirements and had an ST score of 128. (ERB, 29 May 2010 (Encl J1)).

4. (U//~~FOUO~~) Basic Training. PFC Manning attended basic training at Fort Leonard Wood, MO from 5 October 2007 until 6 April 2007. His training lasted six months for a

course that normally takes ten weeks. (Medical Records – PFC Bradley E. Manning (Encl L); MFR FLW VTC, 28 Jan 11 (Encl O7)).

a. (U//~~FOUO~~) Medical Issues. On 12 October 2007, PFC Manning began basic training with C Company, 82d Chemical Battalion. (ERB, 29 May 10 (Encl J)). On 23 October 2007, less than two weeks after beginning his training, PFC Manning was placed in a medical hold status due to (b) (6), (b) (7)(C) (Medical Records – PFC Bradley E. Manning (Encl L); MFR FLW VTC, 22 Jan 11 (Encl O7)). However, PFC Manning was not transferred to the Medical Hold Company. Instead, he remained in C Company, 82d Chemical Battalion (MFR FLW VTC, 22 Jan 11 (Encl O7)) pending a command decision on whether PFC Manning should be allowed to complete his training, be recycled (i.e., transferred) to another Basic Training Company to restart his training, or be medically separated. (MFR FLW VTC, 22 Jan 11 (Encl O7)). During his security clearance interview, PFC Manning indicated he was being separated from the service because (b) (6), (b) (7)(C). (SF 86/Investigator Notes, 6 Dec 07 - 7 Dec 07(Encl N1)). However, there is no documentation to show that a separation action was initiated. PFC Manning's medical records show medical issues, but these were resolved on 12 December 2007 when he was medically released without limitations for continued duty at basic training. (Medical Records – PFC Bradley E. Manning (Encl L)).

b. (U//~~FOUO~~) Pencil Stabbing Incident. On 1 November 2007, while in a medical hold status, PFC Manning allegedly stabbed another trainee in the stomach several times with a pencil. (DA Form 2823, (b) (6), 9 Sep 10 (Encl E37-1)). According to Specialist (SPC) (b) (6), the other trainee was mocking PFC Manning and had placed, contrary to PFC Manning's wishes, objects on PFC Manning's bunk. A verbal altercation turned physical when PFC Manning charged the other trainee, striking him in the stomach with his head and stabbing him with a pencil several times. Although PFC Manning made contact with the other trainee's person, the pencil did not break the skin and did not result in any injury to the trainee. The situation was resolved in short order when other trainees stepped in to separate the two Soldiers. (DA Form 2823, (b) (6), 9 Sep 10 (Encl E37-1)). According to SPC (b) (6), the Drill Sergeants were not informed by the trainees because "if one person had gotten into trouble, everybody would have gotten into trouble." (DA Form 2823, (b) (6), 9 Sep 10 (Encl E37-1)). A review of Fort Leonard Wood records failed to reveal any law enforcement, disciplinary, or other record of the 1 November 2007 incident. (MFR FLW VTC, 22 Jan 11 (Encl O7)).

c. (U//~~FOUO~~) March 2008 Command-Referral to Behavioral Health. PFC Manning was reassigned from C Company, 82d Chemical Battalion to C Company, 2d Battalion, 10th Infantry on 22 January 2008 in order to resume basic training. After his reassignment, PFC Manning's basic training was unremarkable until 28 March 2008, five days before graduation, when he was command-referred to Behavioral Health for "tantrum fits of rage." (Behavioral Health Records, SF 600, pages 3-5, 28 Mar 08 (Encl

M1)). The behavioral health provider found that PFC Manning was [redacted]. The provider [redacted] (Behavioral Health Records, SF 600, pages 3-5, 28 Mar 2008 (Encl M1)). According to Fort Leonard Wood officials, command referrals near the conclusion of basic training were not uncommon. (MFR FLW VTC, 22 Jan 11 (Encl O7)). PFC Manning subsequently graduated on 3 April 2008.

5. (U//~~FOUO~~) Advanced Individual Training.

a. (U//~~FOUO~~) YouTube Video. On 7 April 2008, PFC Manning proceeded from basic training at Fort Leonard Wood, Missouri to Advanced Individual Training (AIT) for MOS 35F (Intelligence Analyst) training, at Fort Huachuca, Arizona, where he was assigned to D Company, 305th Military Intelligence Battalion. (DA Form 2823, [redacted], 25 Aug 10 (Encl E64-1); PFC Manning's ERB (Encl J1)). While at AIT, PFC Manning posted a video to YouTube regarding Sensitive Compartmented Information Facilities (SCIFs) located on Fort Huachuca, Arizona. PFC Manning's video referenced his access to classified material, prompting the chain of command to initiate an inquiry. PFC Manning was counseled on unauthorized disclosure and had to provide training for the unit regarding Operational Security. (MFR, [redacted], 7 Feb 11 (Encl (E93-3); CID Form 94, 10 Sep 10 (Encl E93-1); CID Form 94, 7 Feb 11 (Encl E93-2)). Noncommissioned officers in the unit discussed whether PFC Manning's security clearance should be revoked, but no further action was taken (MFR, [redacted], 7 Feb 11 (Encl (E93-3); CID Form 94, 10 Sep 10 (Encl E93-1); CID Form 94, 7 Feb 11 (Encl E93-2); PFC Manning Joint Adjudication Management Summary (JAMS), 28 Dec 10 (Encl N2)).

b. (U//~~FOUO~~) Unsecured Terminal. There is also some evidence that PFC Manning committed a security violation by leaving a classified computer terminal unsecured. (Email, [redacted], 10 Jan 11 (Encl E60-1)). PFC Manning may have received an Article 15 (non-judicial punishment) while he was at AIT, but there is little evidence that this occurred. When questioned, his AIT company commander thought she remembered some Uniform Code of Military Justice (UCMJ) action associated with PFC Manning, but could not remember what it was for or whether it was a summarized or company grade Article 15. A review of the Fort Huachuca records failed to discover any evidence of nonjudicial punishment pertaining to PFC Manning.[2] (DA Form 2823, [redacted], 25 Aug 10 (Encl E64-1)).

[2] (U//~~FOUO~~) IAW AR 27-10, *Military Justice*, for Soldiers in the grade of E-4 or below, Article 15 (non-judicial punishment actions) are not filed in the Soldier's Official Military Personnel File (OMPF); rather, they are locally filed and maintained for a period of two years or until the Soldier's transfer to another unit or General Court-Martial Convening Authority (GCMCA), whichever occurs first. At the two-year or transfer point, the record is destroyed. See AR 27-10, paragraph(s) 3-16f and 3-37b(1).

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

6. (U//~~FOUO~~) PFC Manning's Time at Fort Drum, August 2008 – October 2009.

a. (U//~~FOUO~~) August 2008 – April 2009. After graduating from AIT, PFC Manning reported to Fort Drum, NY on 28 August 2008. PFC Manning was assigned to the S-2 Section of the 2d Brigade Combat Team. Both PFC Manning's arrival and assignment to 2d Brigade were unremarkable. On 11 September 2008, SSG (b) (6), (b) provided PFC Manning with his "Initial / Integration Counseling." During the counseling, PFC Manning was advised that Staff Sergeant (SSG) (now Warrant Officer One (WO1)) (b) was his platoon sergeant and that all issues were to be handled by either SSG (b) (6), or himself, SSG (b) (6). (DA Form 4856, 11 Sep 08 (Encl K)). Master Sergeant (MSG) (b) (6), (b) (7)(C) was the NCOIC of the S-2 section. On 26 September 2008, PFC Manning received his first adverse counseling for failing a Diagnostic Army Physical Fitness Test (APFT). (DA Form 4856, 26 Sep 08 (Encl K)). PFC Manning was ordered to conduct remedial PT and passed his APFT. (Interview MFR, (b) (7)(C) 29 Jan 11 (Encl E8-4)). On 1 November 2008, PFC Manning was given his monthly counseling for October. While praised for his attitude "entirely devoted towards the S-2 shop success," his inabilities to get to work on time and maintain situational awareness at all times were noted as areas of weakness where he could improve. (DA Form 4856, 1 Nov 08 (Encl K)). Between 1 October 2008 and 5 April 2009, there was no documented evidence of misconduct or failings on PFC Manning's part. (Counseling Packet (Encl K)). In March 2009, MSG (b) (6) changed the supervisory responsibilities of the Noncommissioned Officers (NCOs) in the S-2 section due to the upcoming departure of SSG (b) (6). PFC Manning was placed under the direct supervision of SPC (b) (6), (b) (7)(C) (DA Form 2823, (b) (7)(C) 19 Jan 11 (Encl E78-5)).

b. (U//~~FOUO~~) 6 April 2009 Incident. On 6 April 2009, PFC Manning failed to report to physical training (PT). His direct supervisor, SPC (b) (7)(C) went to his barracks room to wake him up and escort him to MSG (b) (7) While walking to see MSG (b) (7) PFC Manning lost his composure and military bearing by waving his arms and "proceed[ing] with an unruly outburst of screaming to the extent of expelling spit, clenching [his] fist, and shaking in a fury." Observing this behavior, MSG (b) (6) intervened, calmed PFC Manning down and eventually convinced him to voluntarily visit a behavioral health provider (i.e., self-referral to Behavioral Health). (DA Form 4856, 7 Apr 09 (Encl K); DA Form 2823, (b) (7)(C) 19 Jan 11(Encl E78-5); (b) (6) MFR, 21 Dec 09 (E1-1)). On 7 April 2009, PFC Manning was given an adverse counseling for failure to report to PT on time (Failure to Repair - FTR) and disrespect. (DA Form 4856, 7 Apr 09 (Encl K)). Behavioral health records indicate that PFC Manning was first seen by Behavioral Health at Fort Drum on 30 June 2009. (Behavioral Health Records, 30 Jun 09 (Encl M1-2)). Since PFC Manning self-referred, the evaluation by behavioral health providers was not given to the chain of command. During the 30 June 2009 visit, the behavioral health provider did not note any psychiatric abnormalities and did not

require any follow-up, though PFC Manning was told he could return if needed. (Behavioral Health Records, 30 Jun 09 (Encl M1-2)).

c. (U//~~FOUO~~) May through July 2009. In May 2009, Sergeant (SGT) [redacted] became PFC Manning's direct supervisor. When SGT [redacted] went on leave, MSG [redacted] placed SPC [redacted] in charge of PFC Manning. (DA Form 2823, [redacted] 23 Jun 10 (Encl E57-2); Interview MFR, [redacted] 24 Jan 11 (Encl E8-3)). In June of 2009, PFC Manning had conducted himself well enough to be recommended for competition in the August Soldier of the Month Board. His monthly counseling noted "(y)our overall performance has led you to being recommended to compete at the August Soldier of the Month Board." (DA Form 4856, 3 Jun 09 (Encl K)). This counseling statement written by SPC [redacted] is, however, at odds with statements she made during this investigation. (DA Form 2823, 19 Jan 11 (Encl E78-5); DA Form 2823, [redacted] 18 Jun 10 (Encl E78-3)). This recommendation is also at odds with SGT [redacted] overall assessment of PFC Manning. SGT [redacted] said he noted some anomalies and did not think that PFC Manning should deploy. These anomalies included PFC Manning's lack of personal hygiene; that he was a loner and awkward in his interaction with others; that PFC Manning was always the focus of distractions in the S-2 section; and that PFC Manning did not pull his own weight or operate as a Soldier. (Interview MFR, [redacted] 26 Jan 10 (Encl E57-3)). This 15-6 investigation did not uncover any written counseling statements of PFC Manning by SGT [redacted] (Counseling Packet, Encl K).

d. (U//~~FOUO~~) July/August 2009 Incident at the Joint Readiness Training Center (JRTC).[3] During the 2/10 MTN's second rotation[4] at JRTC, PFC Manning was counseled for another FTR. During the counseling, he had another outburst when he slammed a chair down on the ground and ran out of the 2/10 MTN's Tactical Operations Center (TOC). (Interview MFR, [redacted] 20 Jan 11 (Encl E26-3); DA Form 2823, [redacted], 6 Jan 11 (Encl 46-1)). MSG [redacted] again intervened, calming PFC Manning and getting him back on task. This second incident reportedly resulted in another walk-in to behavioral health. (Interview MFR, [redacted] 20 Jan 11 (Encl E26-3)). Behavioral health records confirm that PFC Manning was seen by behavioral health providers at Fort Drum on 19 August 2009. (Behavioral Health Records (Encl M1-3)).

e. (U//~~FOUO~~) Other Pre-Deployment Incidents and Behaviors. According to SPC [redacted] there were several other incidents with PFC Manning prior to the

[3] (U) The Joint Readiness Training Center (JRTC) is focused on improving unit readiness by providing highly realistic, stressful, joint and combined arms training across the full spectrum of conflict (current and future). With great emphasis on realism, the JRTC provides rotational units with the opportunity to conduct joint operations which emphasize contingency force missions. The JRTC training scenario is based on each participating organization's mission essential tasks list and many of the exercises are mission rehearsals for actual operations the organization is scheduled to conduct.
[4] (U) The standard length of a JRTC rotation is approximately three weeks.

deployment. SPC [redacted] noticed that PFC Manning would "freeze emotionally" when corrected or redirected in any way. PFC Manning told her he felt "paranoid," and that "people were listening in on him." PFC Manning also told her that he had no loyalty to the United States and "that the flag on his shoulder meant nothing to him." (DA Form 2823, [redacted] 19 Jan 11 (Encl E78-5)). SPC [redacted] does not remember exactly when PFC Manning made these statements, other than it was in the March - April timeframe. SPC [redacted] also stated that at some point PFC Manning told her he had to "scrub the internet of anything with his name on it or he wouldn't have gotten a security clearance." (DA Form 2823, 19 Jan 11 (Encl E78-5)). SPC [redacted] specifically recalls, however, that she immediately reported the "no loyalty" and the "scrubbing the internet" statements to MSG [redacted] because she did not think the statements were appropriate, especially for a Soldier who had a TS security clearance. SPC [redacted] recalls that she even used the phrase "possible spy" when she reported the statements to MSG [redacted] According to SPC [redacted] she believes that MSG [redacted] brought the "no loyalty to the United States" statement to the attention of Major (MAJ) [redacted], Intelligence Section (S-2) officer in-charge (OIC). (DA Form 2823, [redacted] 19 Jan 11 (Encl E78-5)). The investigation found no other evidence to confirm that MSG [redacted] raised this issue to MAJ [redacted]. (Interview MFR, [redacted], 19 Jan 11 (Encl E15-1)). None of the incidents described above (the 6 April 2009 incident of FTR and disrespect, the JRTC incident, and the statement about "no loyalty to the United States") resulted in any disciplinary actions or a derogatory report to the U.S. Army Central Clearance Facility (CCF). (JAMS, 28 Dec 10 (Encl N2)).

f. (U//~~FOUO~~) Overall Performance. In garrison and pre-deployment, PFC Manning was described as a mediocre Soldier by his peers and supervisors. As noted above, he had issues with being on time. He was also described as having low personal hygiene standards. (DA Form 2823, [redacted] 13 Jan 11 (Encl E47-4); Interview MFR, [redacted] 26 Jan 11 (Encl 57-3); DA Form 2823, [redacted], 19 Jan 11(Encl E16-3)). In contrast, several senior officers in the BCT, including the 2/10 MTN Commander (CDR), Colonel (COL) [redacted] said that PFC Manning was an impressive briefer. (DA Form 2823, [redacted] 20 Jan 11(Encl E56-1); DA Form 2823, [redacted], 25 Jan 11(Encl E92-1)).

7. (U//~~FOUO~~) Decision to Deploy PFC Manning.

a. (U//~~FOUO~~) Discussions Regarding Deploying PFC Manning. Prior to deployment, Chief Warrant Officer Two (CW2) [redacted] recommended to both MAJ [redacted] and MSG [redacted] that PFC Manning not deploy. (Interview MFR, [redacted] 20 Jan 11 (Encl E26-3)). Notwithstanding this recommendation and PFC Manning's previous documented behavioral health and disciplinary issues (i.e., FTR x 2 and disrespect), PFC Manning deployed. The response given to CW2 [redacted] by MSG [redacted] was that since the section was short personnel and PFC Manning had not committed any crimes, he would deploy. (Interview MFR, [redacted] 20 Jan 11 (Encl E26-3)). This comment is confirmed by SPC [redacted] statement wherein she states

that PFC Manning, in essence, had to deploy because "there was nothing on paper that could have proved Manning should have stayed behind." (DA Form 2823, [redacted] 19 Jan 11 (Encl E78-5)).

b. (U//~~FOUO~~) MSG [redacted] S-2 NCOIC. According to MSG [redacted] he personally made the decision to deploy PFC Manning despite the behavioral health issues that had apparently begun to appear (i.e., two prior outbursts and referral to Behavioral Health). (Interview MFR, [redacted] 21 Dec 09 (Encl E1-1)). In a Memorandum for Record, dated 21 December 2009, MSG [redacted] wrote "I decided SPC Manning should deploy given manpower issues and he seemed receptive to possible therapy and/or medication and suffered no other major outbursts." In a statement he provided on 10 June 2010, MSG [redacted] wrote that he and MAJ [redacted] discussed leaving PFC Manning behind. (DA Form 2823, [redacted] 10 Jun 10 (Encl E1-5)).

c. (U//~~FOUO~~) MAJ [redacted], S-2 OIC. When interviewed on 19 January 2011, MAJ [redacted] did not recall talking to MSG [redacted] about leaving PFC Manning at Fort Drum with the rear detachment. MAJ [redacted] was, however, aware of some of PFC Manning's anger management issues and that MSG [redacted] was trying to get SPC Manning behavioral health assistance before the deployment. According to MAJ [redacted], MSG [redacted] dealt with enlisted Soldier issues, but MAJ [redacted] believed that MSG [redacted] kept him in the loop on Soldier issues about 90-95% of the time. MAJ [redacted] does not remember talking to the company commander about SPC Manning and stated that "we didn't take too many issues outside the S-2 shop." (Interview MFR, [redacted], 19 Jan 11, Encl E15-1)).

d. (U//~~FOUO~~) Chain of Command. This investigation revealed no evidence to conclude that anyone in the chain of command, outside the S-2 section, was aware of PFC Manning's behavioral problems. Also, there is no evidence that anyone in the UCMJ/Administrative chain of command was aware that there were concerns about PFC Manning's suitability for deployment. First Sergeant (1SG) [redacted] (HHC, 2/10 MTN), PFC Manning's First Sergeant, confirmed the deployment decision was not raised to Company level. (DA Form 2823, [redacted] 18 Jan 11 (Encl E-82-1); see also, DA Form 2823, [redacted], 5 Jan 11(Encl E85-1)). This is consistent with SPC [redacted] observation that the S-2 section handled everything "internally . . . not telling the company commander" and MAJ [redacted] statement that they, the S-2 section, "didn't take too many issues outside the S-2 shop." (DA Form 2823, [redacted] 19 Jan 11 (Encl E78-5); Interview MFR, [redacted], 19 Jan 11 (Encl E15-1)).

e. (U//~~FOUO~~) Commander's Guidance. The decision by MSG [redacted] to deploy PFC Manning was consistent with pre-established criteria by the Brigade Commander, COL [redacted]. The commander's guidance on non-deployable personnel or personnel returning to Fort Drum from theater was based on two questions: "First, could the Soldier receive the type of care they needed in a deployed environment? Second, was

the Soldier a threat to themselves or others?" If the care was not available in theater or the Soldier was a threat to self or others, the Soldier would not deploy or, if already deployed, would be returned to Fort Drum. (DA Form 2823, [redacted], 20 Jan 11 (Encl E56-1)). MSG [redacted] decided PFC Manning should deploy given manpower issues and because PFC Manning seemed receptive to therapy and medication. Further, PFC Manning did not suffer any further outbursts after the July/August 2009 JRTC rotation. ([redacted] Prepared MFR, 21 Dec 09 (Encl E1-1); DA Form 2823, [redacted], 6 Jan 11 (Encl E20-1)).

(1) (U//~~FOUO~~) 2/10 MTN Mission. COL [redacted] guidance was based on the needs of the Soldiers as well as the needs of the mission. The brigade's mission was to: 1) partner with and train the 1st Federal Police and the 9th Iraqi Army and provide security for the upcoming February 2010 elections; 2) transition to "Iraqi forces in the Lead"; and 3) transfer Joint Security Stations (JSSs) and Combat Outposts (COPs) to Iraqi control after the elections. 2/10 MTN was assuming the authority for a vast expanse of battle space (Eastern Baghdad) and significant number of JSSs and COPs in the brigade's footprint (17 JSSs and COPs). Based on the mission, COL [redacted] determined that 2/10 MTN needed all qualified Soldiers to deploy in support of the mission. (DA Form 2823, [redacted], 20 Jan 11 (Encl E56-1)).

(2) (U//~~FOUO~~) Unit Strength. Prior to deployment, the number of non-deployable Soldiers in 2/10 MTN, at its peak, was 500-600. This number, by the time the 2/10 MTN Brigade fully deployed, was reduced by 50% to approximately 300 personnel. The non-deployables, as COL [redacted] recalls, were "mostly medicals and chapters." (DA Form 2823, [redacted], 20 Jan 11 (Encl E56-1)). The situation in the S-2 shop (i.e., Intelligence Section) was described by COL [redacted] as "pretty thin." The section was operating with two NCOs out of six authorized positions. (DA Form 2823, [redacted], 13 Jan 11 (Encl E47-4)). Although a cross-leveling of noncommissioned officers from the battalion intelligence sections was an option, no such cross-leveling occurred. COL [redacted] decided to assume risk by accepting personnel shortages at the 2/10 MTN level rather than impact the battalions where he believed the personnel were most needed and could provide greater effort to the mission. COL [redacted] noted, "all of my staff was relatively thin, but rather than place inexperienced Intel personnel at the battalions, I chose to accept risk at the Brigade level instead of at more remote locations – particularly in a bottom up, intel-driven fight." (DA Form 2823, [redacted], 20 Jan 11 (Encl E56-1)).

8. (U//~~FOUO~~) Deployment. PFC Manning deployed on 11 October 2009 with 2/10 MTN. During November and December 2009, PFC Manning worked the night shift in the SCIF and was under the direct supervision of first SPC [redacted] and later SPC [redacted]. At this time, PFC Manning's rank was Specialist. (DA Form 2823, [redacted], 13 Jan 11 (Encl E47-4)).

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

a. (U//~~FOUO~~) 12 December 2009 Incident. During the month of December, PFC Manning was counseled by MSG [redacted] for losing his room key. During the counseling, PFC Manning shoved a chair and began yelling. MSG [redacted] calmed him down. ([redacted] Prepared MFR, 21 Dec 2009 (Encl E1-1)). There is no documentation other than MSG [redacted] MFR that any further action, such as a negative counseling or UCMJ action, was taken for PFC Manning's outburst and disrespect in comportment towards an NCO. (Counseling Packet (Encl K); JAMS, 28 Dec 10 (Encl N2)).

b. (U//~~FOUO~~) 18 - 20 December 2009. Between 18 and 20 December, PFC Manning was counseled twice by his supervisor, SPC [redacted], for FTRs. During the second counseling on 20 Dec 2009, PFC Manning screamed and picked up a table, then dropped it causing a government computer screen to break. Despite the apparent damage to Government property, no investigation or action was taken to assess PFC [redacted]'s accountability for the damage. While the incident was brought to 1SG [redacted] attention, this investigation failed to uncover any evidence that damage to Government property was brought to the attention of the company commander, MAJ [redacted] (DA Form 2823, [redacted] 18 Jan 11 (Encl E82-1); Interview MFR, [redacted] 5 Feb 11 (Encl E82-2)). During the incident, PFC Manning moved aggressively towards SPC [redacted] and then moved in the direction of the weapons rack. (Interview MFR, [redacted] 20 Jan 11(Encl E26-3); DA Form 2823, [redacted] 19 Jan 1 (Encl E78-5)). CW2 [redacted] intervened and physically subdued PFC [redacted] before he could get to the weapons rack. (Interview MFR, [redacted] 20 Jan 11 (Encl E26-3); DA Form 2823, [redacted] 19 Jan 11 (Encl E78-5)). Captain (CPT) [redacted] (Assistant S-2) and CPT [redacted] (Assistant S-2-Plans) were both informed of PFC Manning's outburst. (Interview MFR, [redacted] 20 Jan 11 (Encl E26-3)). Separately, CW2 [redacted], the targeting officer, informed 1SG [redacted] about the alleged assault. (Interview MFR, [redacted] 5 Feb 11(Encl 82-2)). In a Memorandum for Record prepared by MSG [redacted] dated 21 December 2009, MSG [redacted] wrote that PFC Manning "stated repeatedly that he does not feel that he has any problems, and therapy will be of little or no value." ([redacted] Prepared MFR, 21 Dec 09 (Encl E1-1)).

(1) (U//~~FOUO~~) 24 December 2009 Command-Referred Behavioral Health Evaluation. Upon hearing about the incident from CW2 [redacted], 1SG [redacted] went to MSG [redacted] to get the full story. (Interview MFR [redacted] 5 Feb 11 (E82-2)). PFC [redacted] was verbally counseled by 1SG [redacted] and was command-referred to behavioral health. (DA Form 2823, [redacted] 18 Jan 11 (Encl E82-1)). On 24 December 2009, PFC [redacted] was seen by CPT [redacted], a licensed clinical psychologist and member of 55th Medical Company. Although PFC Manning was seen on 24 December 2009, CPT [redacted] filed the form documenting his evaluation of PFC Manning on 25 December 2009. (Behavioral Health Records, 25 Dec 09 (Encl M1-1); DA Form 2823, [redacted], 18 Jan 11 (Encl E17-2)).

(a) (U//~~FOUO~~) Evaluation. CPT (b) (6), (b) diagnosed PFC Manning with "(b) (6) [redacted] determined PFC Manning was fit for continued service, and provided some precautionary findings and recommendations regarding danger to others. Specifically, CPT (b) (6), (b) found PFC Manning to be "potentially dangerous" and recommended "removal of weapon (or bolt from weapon) and increased monitoring and supervision." (Behavioral Health Records, 25 Dec 09 (Encl M1-1)). CPT (b) (6), (b) also found that "(c)hapter separation is not recommended at this time but may be considered if his outbursts persist or if he fails a course of treatment." (Behavioral Health Records, 25 Dec 09 (Encl M1-1)). After that incident, PFC Manning began regular psychotherapy. (DA Form 2823, (b) (6), (b) , 18 Jan 11 (Encl E17-2)).

(b) (U//~~FOUO~~) Lack of Security Clearance Finding. CPT (b) (6), (b) filled out a "MEDCOM Form 4038[5]," report of behavioral health evaluation using an unapproved form. Block 7 under "Fitness for Duty and Continued Service permits the behavioral health provider to indicate the Soldier "is not suitable for continued access to classified material and any security clearances should be rescinded." This box was *not checked* on PFC Manning's 25 Dec 09 "MEDCOM Form 4038" completed by CPT (b) (6), (b) . (Behavioral Health Records, 25 Dec 09 (Encl M1)). When interviewed, CPT (b) (6), (b) stated that he did not remember PFC Manning as he only saw him one time and that was over one year ago. Additionally, CPT (b) (6), (b) could not recall the facts and circumstances regarding the lack of any Block 7 entry on PFC Manning's 25 Dec 09 "MEDCOM Form 4038." (Email, (b) (6), (b) 1 Feb 11 (Encl E92-1); Behavioral Health Records, 25 Dec 09 (Encl M1-1)).

(2) (U//~~FOUO~~) No Further Company Command Action. Other than the command referral to behavioral health and the verbal counseling by the First Sergeant, the command took no other action in regards to the 20 December incident. Notwithstanding the alleged disrespect, insubordination, destruction of Government property, and assault by offer, no UCMJ or disciplinary action was pursued against PFC Manning. This investigation found no evidence that MAJ (b) (6) [redacted] conducted any commander's inquiry or investigation of any sort to ensure that he understood the full extent of PFC Manning's misconduct and behavioral health issues. Further, the command did not suspend PFC Manning's access to classified information and did not submit a Report of Unfavorable Information for Security Determination (DEROG) (DA Form 5248-R) to the CCF. (JAMS, 28 Dec 10 (Encl N2); DA Form 2823, (b) (7)(C) 18 Jan 11 (Encl E82-1)).

[5] Although MEDCOM Form 4038 was unapproved, it was used for three command referred evaluations for PFC Manning. This report will continue to refer to the MEDCOM Form 4038. A greater discussion regarding the form appears in the Behavioral Health discussions which follow.

c. (U//~~FOUO~~) January – March 2010. PFC Manning took Environmental/Morale Leave (EML) from 23 January to 11 February 2010. Upon his return, the new 2/10 MTN S-2, CPT [redacted] placed PFC Manning on the day shift where he could be better supervised. During this time, PFC Manning continued to have some problems, such as freezing up during briefings and requiring assistance to remain focused, but he "wasn't as bad as before." (DA Form 2823, [redacted] 19 Jan 11 (Encl E78-5)). SPC [redacted] observed that "PFC Manning had no physical incidents because he was watched." (DA Form 2823, [redacted] 19 Jan 11 (Encl E78-5)). PFC Manning's first line supervisor, SSG [redacted] stated that he consistently monitored PFC Manning's work and behavior. (Interview MFR, [redacted] 24 Jan 11 (Encl E8-3)).

d. (U//~~FOUO~~) Second "No Loyalty" Comment. Sometime in the February or March 2010 timeframe, CW2 [redacted] reports that the Soldiers were sitting around the SCIF and talking about why they joined the Army. PFC Manning said "the U.S. Flag meant nothing to him and he had no loyalties to our country." When asked why he joined our Military he said "because he had no choice." (DA Form 2823, [redacted] 1 Oct 10 (Encl E26-1)). CW2 [redacted] said that at the time "I was concerned not for his patriotism but for him because that could be signs of depression or anger issues." (DA Form 2823, [redacted] 1 Oct 10 (Encl E26-1)). CW2 [redacted] could not recall the exact date of this conversation though he believed that it happened about the time of the Equal Opportunity (EO) complaint. (Interview MFR, [redacted] 2 Feb 11 (Encl E26-5)). CPT [redacted] confirmed an anonymous EO complaint was filed in February-March 2010. (DA Form 2823, [redacted] 13 Jan 22 (Encl E47-4)). SPC [redacted] states that the EO complaint occurred sometime after PFC Manning returned from EML. (DA Form 2823, [redacted] 18 Jan 11 (Encl E78-5)). MSG [redacted], S1 NCOIC, confirmed that PFC Manning was on EML from 23 Jan 10 though 11 Feb 10. (DA Form 2823, [redacted], 5 Jan 11 (Encl E67-1)).

e. (U//~~FOUO~~) April 2010. During April, PFC Manning displayed further unusual behavior – stopping in mid-sentence during conversations, giving blank stares when spoken to and reporting to be in an altered or disassociated state of consciousness. ([redacted] Prepared MFR, 26 Apr 10 (Encl E1-2); the MFR is dated 26 Apr 09 but this is a typographical error).

(1) (U//~~FOUO~~) "My Problem" Email. On 24 April 2010, SPC Manning sent an Email to MSG [redacted] labeled "My problem." Attached to the email was a picture of PFC Manning appearing as a woman, wearing a blond wig and make-up. The email, in part, reads:

> This is my problem, I've had signs of it for a very long time. Its caused problems within my family. . . . Now, the consequences of it are dire, at a time when its causing me great pain in itself. . . . It's destroyed my ties with my family, caused me to lose several jobs, and its currently affecting

> my career . . . . I don't know what to do anymore, and the only 'help' that seems to be available is severe punishment and/or getting rid of me. All I do know, is that fear of getting caught has caused me to go to great lengths to consciously hide the problem. As a result, the problem and the constant cover-up has worn me down to a point where it's always on my mind, making it difficult to concentrate at work, difficult to pay attention to whatever is going on, difficult to sleep, impossible to have any meaningful conversations, and makes my entire life feel like a bad dream that won't end. (Email, Manning, 26 Apr 10 (Encl 013)).

(2) (U//~~FOUO~~) Referral to Chaplain. Following the above noted email, MSG (b) (6) referred PFC Manning to Chaplain (CH) (CPT) (b) (6), (b) (7)(C) on 25 April 2006. In a Memorandum for Record (MFR), dated (mistakenly) 26 April 2009 (the correct year was 2010), MSG (b) (6) references PFC Manning's bizarre behavior and PFC Manning's email of 24 April, but he does not specify the gender issues that PFC Manning discussed. ((b) (6), Prepared MFR, 26 Apr 09 (Encl E1-2)).

(3) (U//~~FOUO~~) Failure to Notify Command. MSG (b) (6) did not inform anyone in the chain of command about the 24 April 2010 email until 4 June 2010. (DA Form 4856, (b) 7 Jun 10 (Encl 47-5)). No action was taken by MSG (b) (6) to inform the chain of command about PFC Manning's situation, thus preventing the chain of command from taking action to command-refer PFC Manning to behavioral health, suspend PFC Manning's access to classified information, initiate a separation action, or submit a DEROG. (DA Form 2823, (b) 2 Jun 10 (Encl E47-5); JAMS, 28 Dec 10 (Encl N2)).

f. (U//~~FOUO~~) 8 May 2010 Assault on Female Supervisor. On 8 May 2010, PFC Manning assaulted his former team leader, SPC (b) (6), (b) in the 2/10 MTN SCIF. (PFC Manning Article 15 Packet, 24 May 10 (Encl J1)).

(1) (U//~~FOUO~~) Prior to the Assault. On 7 May 2010 around 1830, PFC Manning left an informal section meal. MSG (b) (6) found PFC Manning an hour later in a storage room in a fetal position. PFC Manning was sitting upright with his knees tucked under his chin obviously agitated about something. He was clutching his head with his eyes clenched shut. MSG (b) (6) noticed a folding chair with cut marks on the padded seat with the words "I want" etched on the seat. There was an open knife at PFC Manning's feet and several cut pieces of vinyl. Initially, PFC Manning was not responsive to MSG (b) (6) Eventually, PFC Manning began to respond and stated that the calm person who was speaking was a personality independent of the person sitting on the floor in obvious pain. PFC Manning drew the analogy of him being a turtle with a core personality, and several layers of hardened shell, fragmented and designed to protect the core personality, and functioning in different situations as the need required. After spending time with him, MSG (b) (6) determined that PFC Manning had recovered

sufficiently to finish the last four hours of his shift. ([redacted] Prepared MFR, 8 MAY 10 (Encl E1-2)).

(2) (U//~~FOUO~~) The Assault. After PFC Manning returned to complete the rest of his shift, he assaulted SPC [redacted] SPC [redacted] had been called back to the SCIF to address a targeting issue. Upon entry into the SCIF, she asked the other Soldiers what they had done regarding the search for the information she was requested to locate. PFC Manning told SPC [redacted] he had already conducted the search for information she was engaged in and also told her not to berate Soldiers in the SCIF. (PFC Manning Article 15 Packet, 24 May 10 (Encl J1); DA Form 2823, [redacted] 19 Jan 11 (Encl E78-5)). SPC [redacted] replied with, "Manning how about you get your shit together before you tell me how to fix mine." PFC Manning yelled "no" and ran at SPC [redacted] punching SPC [redacted] in the face and slamming his body into hers. In self-defense, SPC [redacted] pinned PFC Manning down and screamed at him "is this what you want." (DA Form 2823, [redacted] 19 Jan 11 (Encl E78-5)). CPT [redacted] First Lieutenant (1LT) (then Second Lieutenant (2LT)) [redacted] and SPC (then PFC) [redacted] all witnessed the assault by PFC Manning and separated the two Soldiers. SPC [redacted] was unaware of whether any of the SCIF personnel, at that time, took action to inform the chain of command. (DA Form 2823, [redacted] 19 Jan 11 (Encl E78-5)).

(3) (U//~~FOUO~~) Report to Command. The following morning, 1LT [redacted] who was assigned to the S-2 section in March 2010, was informed of PFC Manning's assault on SPC [redacted] Shortly thereafter, 1LT [redacted] observed PFC Manning, still in possession of his weapon, walking with MSG [redacted] (DA Form 2823, [redacted] 19 Jan 11 (Encl E33-1)). Fearing for the safety of the personnel in the S-2 section, 1LT [redacted] contacted the brigade judge advocate and the new Company Commander, CPT [redacted] informing them both of PFC Manning's assault on SPC [redacted] The military police (MPs) were summoned and PFC Manning was taken away from the SCIF area. The combination to the cipher lock to the SCIF was changed. (DA Form 2823, [redacted] 19 Jan 11 (Encl E33-1)).

(4) (U//~~FOUO~~) Command Response. The command immediately removed PFC Manning's bolt from his weapon and assigned him to duty in the supply room. (DA Form 2823, [redacted] 7 Jan 11 (Encl E32-3)). Additionally, the combination on the SCIF door was changed to preclude PFC Manning from returning. (DA Form 2823, [redacted] 19 Jan 11 (Encl E3-1)).

g. (U//~~FOUO~~) Article 15 and Initiation of Separation Action. Shortly after the assault on SPC [redacted] the process was begun to discipline PFC Manning via a Company Grade Article 15. The Article 15 was completed on 24 May 2010. PFC Manning was reduced from the rank of SPC to PFC and forfeited $446 pay for one month. (PFC Manning Article 15 Packet, 24 May 10 (Encl J1)). Additionally, the chain of command

contemplated separation. (DA Form 2823, (b) (6), (b) 7 Jan 11 (Encl E32-3); DA Form 2823, (b) 19 Jan 11 (Encl E33-1); DA Form 2823, (b) (6), (b) 19 Jan 11 (Encl E78-5)).

h. (U//~~FOUO~~) Derogatory Report. On 9 May 2010, the Company Commander, CPT (b) (6), (b) completed a Report of Unfavorable Information for Security Determination (DEROG Report), DA Form 5248-R recommending temporary revocation of PFC Manning's clearance "until a determination can be made as to the state of his behavioral health." (DA Form 5248-R, 9 May 10 (Encl N5)). The basis for the action was "Assault and Battery." (PFC Manning Article 15 Packet, 24 May 10 (Encl J1)). The DEROG was forwarded to the security manager at division, however, it was returned for additional information. When returned to the Division on its second iteration, the report on PFC Manning was not processed within the required AR 380-67 timeframe because PFC Manning had already been apprehended for his alleged unauthorized disclosure of classified and sensitive information and the Division believed that his clearance was "'out of [the Division's] hands'." (DA Form 2823, (b) (6), 20 Jan 11 (Encl E56-1); DA 2823, (b) (6), 10 Jun 10 (Encl E1-5)).

i. (U//~~FOUO~~) 22 May 2010 Behavioral Health Evaluation. On 22 May 2010, PFC Manning was seen by Behavioral Health for a potential misconduct separation action at the direction of the company commander IAW AR 635-200, Active Duty Enlisted Administrative Separations. (Behavioral Health Records, 22 May 2010 Eval (Encl M1-27)).

(1) (U//~~FOUO~~) Diagnosis. The behavioral health provider, CPT (b) (6), (b) (7)(C), diagnosed PFC Manning (b) (6), (b) (7)(C) and cleared PFC Manning for "expeditious administrative separation." CPT (b) (6), (b) also noted: "(b) (6), (b) (7)(C) CPT (b) (6) considered PFC Manning (b) (6), (b) (7)(C) Therefore, it is recommended that he not have access to a firearm or go on off the FOB missions." (Behavioral Health Records, 22 May 2010 Eval (Encl M1-27)).

(2) (U//~~FOUO~~) Lack of Security Clearance Finding on "MEDCOM Form 4038." When CPT (b) (6), (b) was interviewed regarding the completion of the 22 May 2010 "MEDCOM Form 4038" and the absence of any comment pertaining to PFC Manning's suitability for access to classified information or retention of a clearance, he noted that the block which read "The Service member is not suitable for continued access to

classified material and any security clearances should be rescinded" (Block 7) was intentionally removed by him to increase the space for the write-up under "Other." CPT (b) (6), (b) noted that he thought the access to classified information issue was "moot" because CPT (b) (6), (b) had been advised, by PFC Manning's commander, that PFC Manning was removed from the SCIF at the time of his evaluation. CPT (b) (6), (b) further stated that even if Block 7 on "MEDCOM Form 4038" was not deleted, he would not have recommended suspension of PFC Manning's security clearance based on his 22 May 2010 evaluation. (Interview MFR, (b) (6), (b), 25 Jan 11 (Encl E17-3)).

j. (U//~~FOUO~~) PFC Manning's Apprehension by CID. On 27 May 2010, PFC Manning was apprehended by the U.S. Army Criminal Investigation Command (commonly referred to as CID) for his alleged unauthorized disclosure of classified information to Wikileaks. (DA Form 2823, (b) (6), (b) 11 Jun 10 (Encl E13-2); Search authorization (Encl O33)).

k. (U//~~FOUO~~) Road to Wikileaks. Below at Figure 1 is a pictorial description of significant dates and events leading up to, and including, PFC Manning's apprehension for alleged compromise of classified information.

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

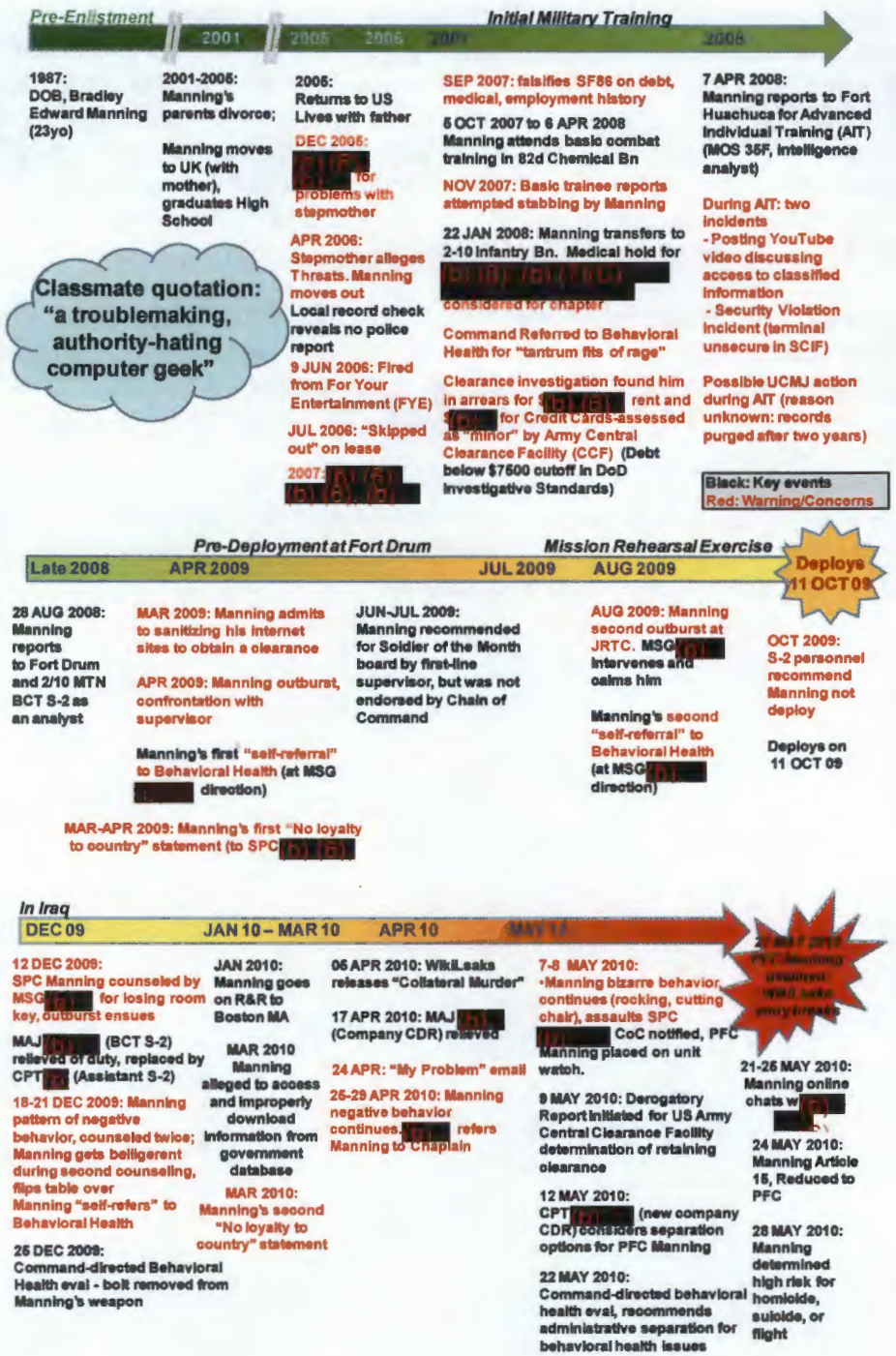

Figure 1: Timeline of events, PFC Bradley Manning. (U//~~FOUO~~)

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

Section IB: Chain of Command

1. (U//~~FOUO~~) Facts Pertaining to the Chain of Command. The following section sets out PFC Manning's supervisory chain, as well as his chain of command. The supervisory chain was responsible for the day-to-day supervision of PFC Manning. However, the chain of command, specifically the company commander, has the ultimate responsibility for ensuring good order and discipline within his company and is vested with command authority under the UCMJ. (AR 600-20, *Army Command Policy*, paragraph 1-5 (Encl Q67)).

a. (U//~~FOUO~~) Pre-deployment. Figure 2 sets out PFC Manning's supervisory chain and his chain of command prior to 2/10 MTN's deployment in October 2009.

(1) (U//~~FOUO~~) Squad Leaders/First-Line Supervisors. PFC Manning's pre-deployment squad leaders were as follows: SSG [redacted] from August 2008 - February 2009; SPC [redacted] from March 2009 - April 2009; and SGT [redacted] from May 2009 - October 2009. As set out in section IA above, both SPC [redacted] and SGT [redacted] noted that PFC Manning had issues and did not think he should deploy with the unit. (Interview MFR, [redacted] 29 Jan 11 (Encl E57-3); DA Form 2823, [redacted] 19 Jan 11 (Encl 78-5)).

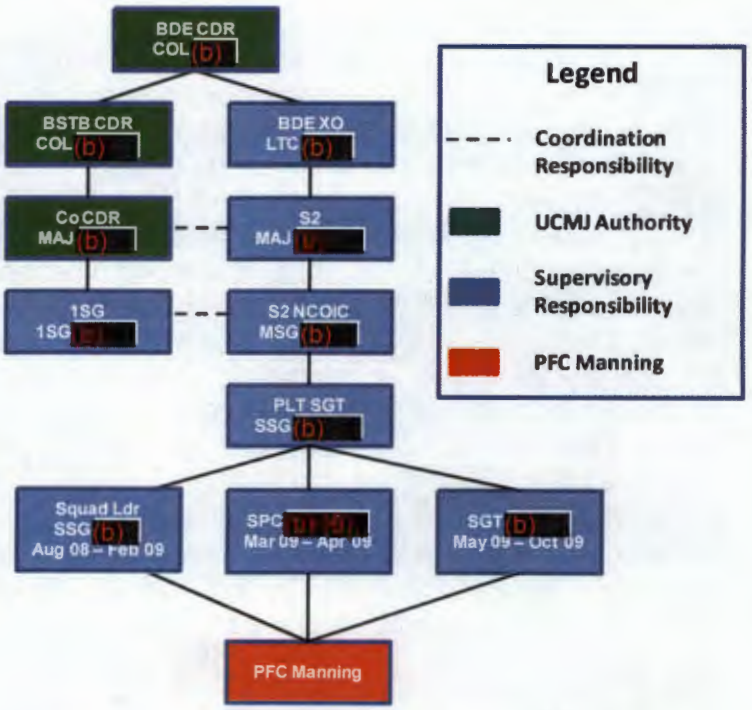

Figure 2. Pre-deployment Supervisory Chain of Command (U//~~FOUO~~)

(2) (U//~~FOUO~~) Platoon Sergeant/Second-Line Supervisors. SSG [redacted] was PFC Manning's platoon sergeant from August 2008 until April 2009 when he was replaced by SGT [redacted] (DA Form 2823, [redacted] 18 Jan 11 (Encl E8-2)). Prior to the deployment, SSG [redacted] resumed his responsibilities as PFC Manning's platoon sergeant. (DA Form 2823, [redacted] 13 Jan 11 (Encl E47-4); DA Form 2823, [redacted] 6 Jan 11 (Encl E46-1)). PFC Manning was a Shia analyst in the SCIF and was supervised by SSG [redacted] and CW2 [redacted] (DA Form 2823, [redacted] 20 Jan 11 (Encl E56-1)). In December 2009, SSG [redacted] was

consulted by SPC [redacted] regarding PFC Manning's continued practice of reporting late to work. SSG [redacted] and MSG [redacted] gave SPC [redacted] permission to counsel PFC Manning for the behavior. (DA Form 2823, [redacted] 21 Jan 11 (Encl E65-1)). CPT [redacted] stated that SSG [redacted] was the best overall analyst in the S-2 section but that SSG [redacted] was lacking in leadership skills. CPT [redacted] indicated that when SSG [redacted] was accepted for the Warrant Officer program, SSG [redacted] "checked out as a leader." (DA Form 2823, [redacted] 13 Jan 11 (Encl E47-4)). CPT [redacted] further stated that he sometimes wished SSG [redacted] was a better leader than analyst because "these Soldiers needed more leadership." (DA Form 2823, [redacted] 13 Jan 11 (Encl E47-4)). It was SGT [redacted] opinion that SSG [redacted] preferred not to be engaged with Soldier issues. (Interview MFR, [redacted] 26 Jan 11(Encl E57-3)). SSG [redacted] departed the unit in May 2010 to attend Warrant Officer Candidate School. (DA Form 2823, [redacted] 13 Jan 11 (Encl E47-4)).

(3) (U//~~FOUO~~) S-2 Section NCOIC, MSG [redacted] As the S-2 NCOIC, MSG [redacted] served as a senior enlisted supervisor for PFC Manning. MSG [redacted] appeared to be aware of every instance of alleged misconduct, behavioral health issue and anomalous behavior by PFC Manning. ([redacted] Prepared MFR, 21 Dec 09 (Encl E1-1); [redacted] Prepared MFR, 26 Apr 09 (Encl E1-2); [redacted] Prepared MFR, 8 May 10 (Encl E1-3)). However, the evidence indicates that MSG [redacted] failed in his duty to inform the chain of command of the true nature and extent of the problems with PFC Manning. (Interview MFR, [redacted] 19 Jan 11 (Encl E15-1); DA Form 2823, [redacted] 20 Jan 11 (Encl E23-2)). MSG [redacted] also failed to conduct the necessary counseling or pursue, through the command, appropriate administrative actions or non-judicial punishment. As the NCOIC, MSG [redacted] changed the supervisory scheme for Soldiers several times pre- and post-deployment. (DA Form 2823, [redacted] 19 Jan 11 (Encl E78-5); Interview MFR, [redacted] 26 Jan 11 (Encl E57-3); DA Form 2823, [redacted] 18 Jan 11 (Encl E8-2); DA Form 2823, [redacted] 19 Jan 11 (Encl E65-1). In addition to the continuous changes in the S-2 mid-level supervisory chain, MSG [redacted] purposefully removed or impeded other NCOs and Warrant Officers from participating in the decision making process, usurping their supervisory responsibilities over enlisted Soldiers within the section. (DA Form 2823, [redacted] 24 Jan 11 (Encl E26-4); DA Form 2823, [redacted] 24 Jan 11 (Encl E8-3); DA Form 2823, [redacted] 18 Jan 11 (E28-2); DA Form 2823, [redacted] 19 Jan 11 (E16-1); DA Form 2823, [redacted] 18 Jan 11 (E8-2); DA Form 2823, [redacted] 21 Jan 11 (E43-1)). When the decision was made to remove CW2 [redacted] from the supervisory chain, CW2 [redacted] brought the issue to the attention of MAJ [redacted] MAJ [redacted] supported both MSG [redacted] decision and the revised supervisory scheme. (DA Form 2823, [redacted] 24 Jan 11 (Encl E26-4)). This supervisory scheme/structure resulted in a dysfunctional supervisory relationship among S-2 mid-level leaders and enlisted Soldiers.

(4) (U//~~FOUO~~) S-2, MAJ [redacted] As the S-2 Section OIC, MAJ [redacted] had supervisory responsibilities over the Soldiers in the section. MAJ [redacted] stated that MSG [redacted] took care of enlisted issues, but kept him informed on most issues. MAJ [redacted] indicated that he knew that PFC Manning had anger management issues and that MSG [redacted] had been trying to get him behavioral health assistance prior to the deployment. MAJ [redacted] does not remember ever discussing with MSG [redacted] whether PFC Manning should be deployed. (DA Form 2823, [redacted] 19 Jan 11 (Encl E15-1)).

(5) (U//~~FOUO~~) Chain of Command. The chain of command began with MAJ [redacted] and 1SG [redacted] The Battalion Commander was COL (then Lieutenant Colonel (LTC)) [redacted] and the Brigade Commander was COL [redacted] This AR 15-6 Investigation did not reveal any evidence that any member of the chain of command was notified about any derogatory information, misconduct or behavioral health issue pertaining to PFC Manning during the period of September 2008 through October 2009 (i.e., the pre-deployment period). (DA Form 2823, [redacted] 19 Jan 11 (Encl E15-1); DA Form 2823, [redacted] 20 Jan 11 (Encl E23-2); DA Form 2823, [redacted] 18 Jan 11 (Encl 82-1); DA Form 2823, [redacted] 5 Jan 11 (Encl E85-1); DA Form 2823, [redacted] 20 Jan 11 (Encl E56-1)).

b. (U//~~FOUO~~) Deployment. During the deployment, PFC Manning's supervisory chain changed frequently. However, the one constant was MSG [redacted] who continued to serve as the NCOIC of the S-2 Section. Figure 3 below provides a pictorial of PFC Manning's deployment technical and UCMJ/Administrative Action chains of command. Figure 4 provides an organizational chart depicting the entire S-2 Section during the deployment and all other periods relevant to this investigation.

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

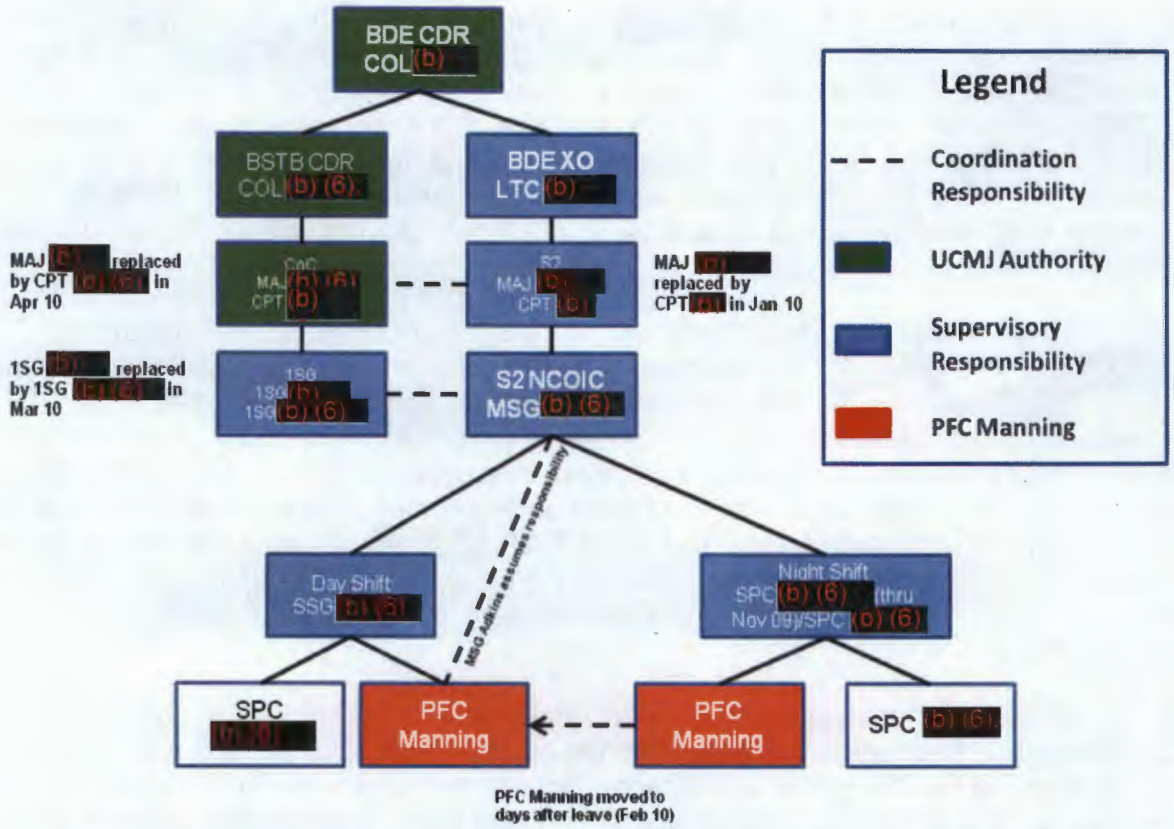

Figure 3. Deployment Supervisory Chain and Chain of Command (U//~~FOUO~~)

(1) (U//~~FOUO~~) Initial Supervisory Chain. As noted in Figure 3 above, SSG (b) (6) had supervisory responsibility over PFC Manning during the unit's forward movement from Fort Drum to Iraq. (DA Form 2823, (b) (6) 23 Jun 10 (Encl E57-2); DA Form 2823, (b) (6) 20 Jan 11 (Encl E56-1)). The supervisory chain of command changed almost immediately upon the unit's arrival in Iraq. SPC (b) (6) (b) PFC Manning's garrison Team Leader from March 2009 to April 2009, was once again designated PFC Manning's direct supervisor. (DA Form 2823, (b) 13 Jan 11 (Encl E47-4)). Within one month, SPC (b) (6) (b) was moved to another position. In November 2009, SPC (b) (6) (b) (7) became PFC Manning's immediate night shift supervisor. (DA Form 2823, (b) 13 Jan 11 (Encl E47-4); DA Form 2823, (b) (6) 21 Jan 11 (Encl E65-1)). SPC (b) (6) states that "I was the pseudo-NCOIC, while I was at Brigade, I was the night shift NCOIC but I was constantly getting pulled to Baghdad as an LNO. In the beginning there really wasn't anyone. CPT (b) was the night OIC and then below me was SPC Manning and SPC (b) (6) (DA Form 2823, (b) (6) 21 Jan 11 (Encl E65-1)). In the absence of SPC (b) (6) SSG (b) (6) was PFC Manning's supervisor. (DA Form 2823, (b) 13 Jan 11 (Encl E47-4)).

(2) (U//~~FOUO~~) Night Shift OIC. In November 2009, CPT [redacted] was made the SCIF night shift OIC, responsible for SPC [redacted] SPC [redacted] and PFC Manning. (DA Form 2823, [redacted] 7 Jan 11 (Encl E44-2)). While not sure of the exact duration, CPT [redacted] remained night shift OIC for no more than five weeks and possibly as few as three weeks before being moved to a subordinate battalion in December 2009. (DA Form 2823, [redacted] 7 Jan 11(Encl E44-2)). After CPT [redacted] movement to battalion, there was no officer on the night shift. (DA Form 2823, [redacted] 7 Jan 11 (Encl E44-2)). In response to the question regarding a night shift NCOIC during his time as OIC, CPT [redacted] noted: "That's a great question. I walked in there and it was like let's just have the bare bones on the night shift. Everything S-2 related primarily happened during the day so that is where the effort was focused." (DA Form 2823, [redacted] 7 Jan 11 (Encl E44-2)). At no time during the deployment did the night shift have any NCO leadership. In fact, CPT [redacted] switched MSG [redacted] to a swing shift so there would be NCO leadership overlapping day and night. (DA Form 2823, [redacted] 13 Jan 11 (Encl E47-4)). A common theme across all investigative interviews was that the night shift was without senior leadership because the mission essential and critical intelligence gathering, analysis and product development occurred during the day shift. (DA Form 2823, [redacted] 7 Jan 11 (Encl E44-2)).

(3) (U//~~FOUO~~) Change in BCT S-2. MAJ [redacted] was the OIC for the S-2 Section until January 2010 when he was removed from his position as S-2 and reassigned to a transition team. (DA Form 2823, [redacted] 20 Jan 11 (Encl E56-1)). MAJ [redacted] was replaced by his Assistant S-2, CPT [redacted] (DA Form 2823, [redacted] 13 Jan 11 (Encl E47-4); DA Form 2823, [redacted] 5 Jan 11 (Encl E85-1); Interview MFR, [redacted] 10 Jan 11 (Encl E45-1)). At that time, CPT [redacted] had three assigned duties: Brigade S-2; Brigade Assistant S-2; and Military Intelligence Company Commander. (DA Form 2823, [redacted] 13 Jan 11 (Encl E47-4); DA Form 2823, [redacted] 18 Jan 11 (Encl E53-3)). CPT [redacted] position of Assistant S-2 was not filled immediately, requiring CPT [redacted] to fulfill both duties. CPT [redacted] eventually assumed the Assistant S-2 duties after several weeks had passed. CPT [redacted] did not give up command of the Military Intelligence Company until 13 January 2010. (ORB, [redacted] 24 Jan 11 (Encl O19)). Upon PFC Manning's return from EML on 11 February 2010, CPT [redacted] placed PFC Manning on the day shift so that PFC Manning could have more NCO supervision and leadership. (DA Form 2823, [redacted] 13 Jan 11 (Encl E47-4)). SSG [redacted] was responsible for PFC Manning while he was assigned to the day shift. (Interview MFR, [redacted] 24 Jan 11 (Encl E8-3); DA Form 2823, [redacted] 6 Jan 11 (Encl E46-1); DA Form 2823, [redacted] 13 Jan 11 (Encl E47-4)). CPT [redacted] went on EML in April 2010 and did not return until after PFC Manning's assault on SPC [redacted] (DA Form 2823, [redacted] 13 Jan 11 (Encl E47-4)). When CPT [redacted] went on leave to the United States, PFC Manning was returned to the night shift, ultimately assaulting SPC [redacted] during one such shift. (DA Form 2823, [redacted] 19 Jan 11 (Encl E78-5)).

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

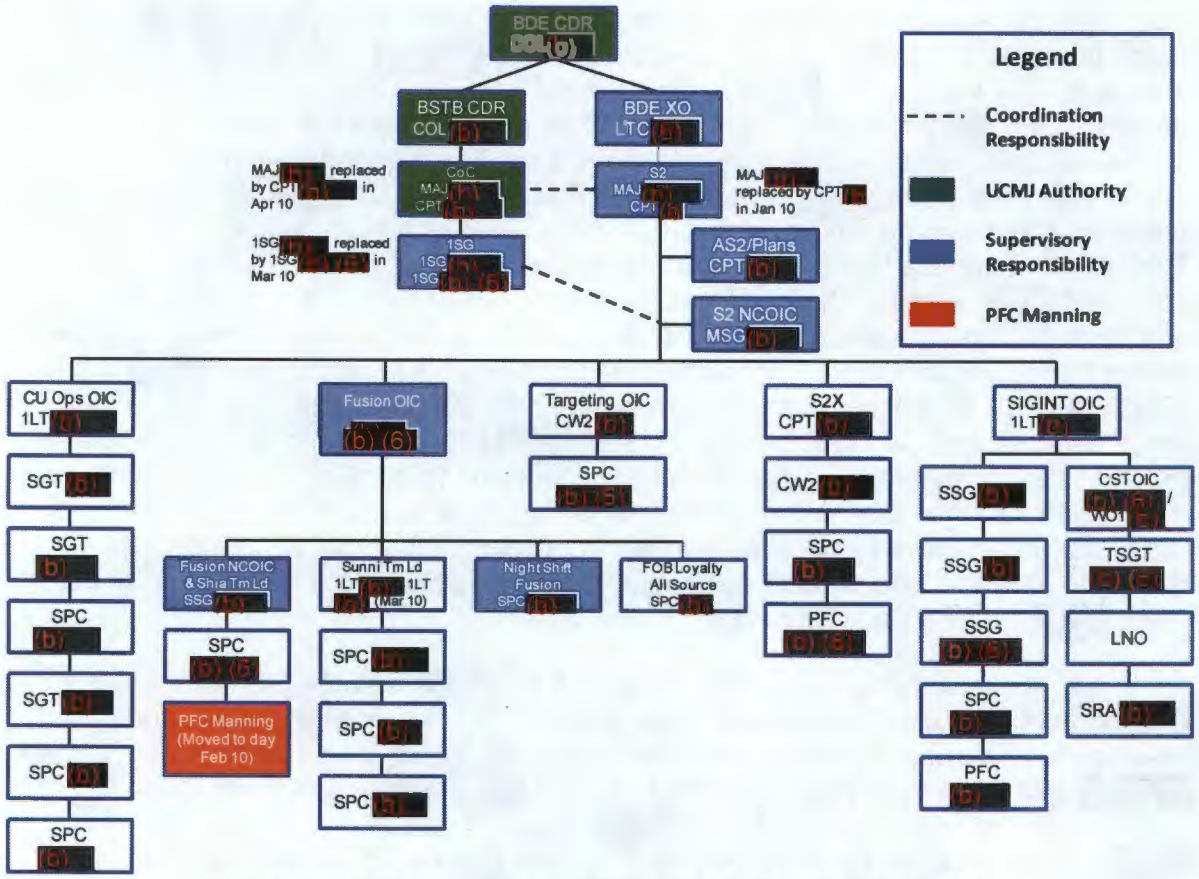

Figure 4. S-2 Organization After January 2010 (U//~~FOUO~~)

(4) (U//~~FOUO~~) March 2010 Supervisory Changes. The final major change in technical leadership within the SCIF was execution of a swing shift plan involving the NCO leadership, specifically MSG (b) (6). On or about March 2010, CPT (b) placed MSG (b) (6) on a swing shift, allowing for NCO leadership overlap between day and night shifts, and providing structure and supervision for the night time S-2 (SCIF) personnel. About this time, MSG (b) (6) personally assumed primary administrative supervision of PFC Manning, relegating SSG (b) (6) (b) role to that of production and quality control of PFC Manning's work product. SSG (b) (6) left the unit in May 2010 to attend the Warrant Officer Basic Course. (DA Form 2823, (b) 13 Jan 11 (Encl E47-4)).

(5) (U//~~FOUO~~) Company Command. On 17 April 2010, MAJ (b) (6) was replaced by CPT (b) (6), (b) as the Headquarters and Headquarters Company (HHC), 2/10 MTN Company Commander. (b) (5), (b) (7)(C) , 17 Apr 10 (Encl O6); DA Form 2823, (b) (6), (b) 7 Jan 11 (Encl E32-3)).

c. (U//~~FOUO~~) BCT Commander's Efforts at Understanding the Unit.

(1) (U//~~FOUO~~) COL (b) (6) implemented several methods of obtaining information about Soldiers within 2/10 MTN. All command directed behavioral health referrals were required to be briefed to COL (b) (6) by battalion commanders as a matter of routine (DA Form 2823, (b) (6) 20 Jan 11 (Encl E56-1)). In fact, during the deployment, there were a total of 24 command referred behavioral health evaluations, resulting in "approximately 16" Soldiers being returned to the United States or delayed from returning to Iraq from EML in the United States. (DA Form 2823, (b) (6) 20 Jan 11 (Encl E56-1)).

(2) (U//~~FOUO~~) Additionally, in January 2010, COL (b) (6) conducted a 100-day review of 2/10 MTN in order to understand his unit and any issues that impacted the unit personnel. COL (b) (6) was seeking knowledge and information about his unit so that he could have better situational awareness of unit stressors, unit stress relievers, Soldier recommendations to their leaders, Soldier climate assessments and the prevalence of depression symptoms among the unit personnel. (DA Form 2823, (b) (6) 20 Jan 11 (Encl E56-1)).

(3) (U//~~FOUO~~) Finally, COL (b) (6) was engaged and involved with 2/10 MTN staff primaries during nightly updates, and received more in-depth staff updates biweekly. (DA Form 2823, (b) (6) 20 Jan 11 (Encl E56-1)). He put into place a leadership structure that gave the executive officer direct oversight and supervisory responsibility for staff sections, including the S-2 and S-6 sections. (DA Form 2823, (b) (6) 20 Jan 11 (Encl E56-1); DA Form 2823, (b) (6) 10 Jan 11 (Encl E45-1)).

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

Section IC: Personnel Security (Security Clearance)

1. (U//~~FOUO~~) Regulations and Policies Pertaining to Personnel Security (Security Clearances). The starting reference for the Army's Personnel Security Program is AR 380-67, *Personnel Security Program*, dated 9 September 1988. AR 380-67 parallels DoD 5200.2-R, *Personnel Security Program*, January 1987. In addition to these two policies, the national investigative and adjudicative standards found in DCID 6/4, *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information*, 2 July 1998 (Encl Q28) and Intelligence Community Directive (ICD) 704, *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information*, 1 October 2008 (Encl Q62), are applicable to the security clearance process. The following paragraphs discuss the standards set out by these policies.

a. (U//~~FOUO~~) Overall Process. Once an applicant has been deemed suitable for military service, there are five important steps in obtaining access to classified information. First, the applicant must submit an application for security clearance using an electronic questionnaire (e-QIP) which electronically produces an SF 86. Second, a security clearance investigation must be conducted by the Office of Personnel Management (OPM). Third, adjudication and determination of the individual's eligibility is conducted by the U.S. Army Central Clearing Facility (CCF). Fourth, access is granted by the local command. Finally, evaluation of eligibility continues—Soldiers and leaders have the responsibility to report derogatory information for individuals with security clearances. (Army G-2 MFR, 28 Jan 11 (Encl O4); AR 380-67, 9 Sep 88 (Encl Q23)). The first three steps determine whether a person is eligible to have access to classified information. The last two steps are critical to ensuring that access is given to the right individuals. The granting of access by the local command requires commanders and supervisors to determine, based on what they know about the individual and the duties assigned, whether the person should be granted access to classified information.

b. (U//~~FOUO~~) Security Clearance Process.

(1) (U//~~FOUO~~) Application. As a general rule, an applicant applies for a security clearance after it is determined there is a need for the applicant to have one. Every 35F Intelligence Analyst is required to have a TS/SCI clearance. To apply, the applicant completes the electronic questionnaire (e-QIP). The applicant must answer all questions on the e-QIP honestly and completely to the best of his knowledge. Like all applicants, PFC Manning completed an e-QIP questionnaire. (Manning's e-QIP Form (Encl N-3)).

(2) (U//~~FOUO~~) Investigation. Because PFC Manning's MOS of 35F required a TS/SCI, the investigation process included a Single Scope Background Investigation (SSBI). (DA Pam 611-21, Chapter 10, 22 Jan 07 (Encl Q32)). The SSBI is conducted by OPM, which applies the National Investigative Standards. The SSBI can cover a period up to 15 years and no less than two years. (AR 380-67, appendix B-4a, 9 Sep 88 (Encl Q-23)). Three notable limitations regarding SSBIs are: (1) a prohibition on investigation into a person's activities prior to his 16th birthday; (2) a prohibition against investigation in a foreign country outside of a military installation; and (3) a prohibition against non-consensual review of an individual's cyber behavior (e.g., use of social networking websites) as part of the security clearance process. (Army G-2 MFR, 28 Jan 11 (Encl O4)). Currently, an individual's cyber behavior is not checked during the security clearance investigative and adjudicative process because legal and privacy limits have not been clearly defined. (Email, (b) (6), (b) 1 Feb 11 (O19)). Because the Army's demographic includes many young Soldiers, security clearance investigations often cover a shorter period of time. (Army G-2 MFR, 28 Jan 11 (Encl O4)). While this poses some risks, the overwhelming majority of these Soldiers have proven that they are not a security risk.

(3) (U//~~FOUO~~) Adjudication. Once the investigation is completed, it is forwarded to the Army CCF for adjudication and determination of the individual's eligibility for TS/SCI access. "The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is an acceptable security risk. . . . The adjudication process is the careful weighing of a number of variables known as the whole-person concept." (Intelligence Community Policy Guidance Number (No.) 704.2, Annex A, part II, 2 Oct 08 (Encl Q49)). CCF must follow the National Adjudicative Guidelines along with their associated mitigation factors. Mitigation is a part of the adjudication process where the nature and extent of a "red flag" is examined in order to determine whether the "red flag" should be considered in determining a person's eligibility for a security clearance. (Army G-2 MFR, 28 Jan 11 (Encl O4)). The 13 adjudicative guidelines and the mitigation factors are listed in the Intelligence Community Policy Guidance No. 704.2, dated 2 October 2008 and an Under Secretary of Defense Memorandum, SUBJECT: Implementation of Adjudicative Guidelines for Determining Eligibility For Access to Classified Information (December 29, 2005), dated 30 August 2006. (Encls 49 and 48, respectively). Mitigation factors include offsetting a person's debt if the amount of debt does not exceed a certain threshold amount. The DoD acceptable debt standard is $7,500. (Army G-2 MFR, 28 Jan 11 (Encl O4)).

(4) (U//~~FOUO~~) Granting Access. Notwithstanding the granting of a security clearance, the local command must still decide whether to grant access to a person with a security clearance. The command obligation regarding access is a continuing duty. When faced with credible derogatory information, commanders must decide whether to

suspend an individual's access to classified information pending the resolution of the issue or the final adjudication of a formal derogatory report to CCF. The decision to suspend is within the commander's discretion. (AR 380-67, paragraph 8-102(a), 9 Sep 88 (Encl Q23); Army G-2 MFR, 28 Jan 11 (Encl O4)).

(5) (U//~~FOUO~~) Evaluating Continued Security Eligibility. DoD 5200.2-R and AR 380-67 establish continuing security responsibilities for commanders, supervisors, individuals and co-workers. Both regulations state "the issuance of a personnel security clearance or the determination that a person is suitable for assignment to sensitive duties cannot be considered as a final personnel security action . . . . [T]he individual's trustworthiness is a matter of continuing assessment." (DoD 5200.2-R, paragraph C9.1.1, 2 Feb 96, as amended by OSD Memo "Personnel Security Investigations and Adjudications, 10 Nov 98 (Encl Q31); AR 380-67, paragraph 9-100, 9 Sep 88 (Encl Q23)).

(a) (U//~~FOUO~~) Reasons for Derogatory Report. AR 380-67, paragraph 2-200, provides a list of potential behaviors that could result in derogatory reports. These include criminal conduct; acts of omission or commission that indicate poor judgment, unreliability, or untrustworthiness; and any behavior or illness, including any mental condition, which, in the opinion of competent medical authority, may cause a defect in judgment or reliability with due regard to the transient or continuing effect of the illness and the medical findings in such case. (AR 380-67, paragraph 2-200, 9 Sep 88 (Encl Q23)).

(b) (U//~~FOUO~~) Requirement for Personnel and Commanders to Report. "Whenever derogatory information relating to the criteria and policy set forth in paragraph 2-200 and appendix I (the Army adjudication policy) is developed or otherwise becomes available, it shall be referred by the most expeditious means to the commander or the security officer of the organization to which the individual is assigned for duty." (AR 380-67, paragraph 8-101, 9 Sep 88 (Encl Q23)). Appendix I of AR 380-67 lists the old adjudication criteria for security clearances which were updated in 2006. Guideline A of the current adjudication policy references an individual's allegiance to the United States. "When the commander learns of credible derogatory information on a member of his or her command that falls within the scope of paragraph 2-200, the commander will immediately forward DA Form 5248-R (See Encl Q34) to the Commander, CCF." (AR 380-67, paragraph 8-101, 9 Sep 88 (Encl Q23)). Neither DoD 5200.21-R nor AR 380-67 make a failure to report derogatory information a punishable offense under the UCMJ.

c. (U//~~FOUO~~) Training Requirements. DoD 5200.2-R, paragraphs C9.1.3 (Encl Q34) and AR 380-67, paragraph 9-101, 9 Sep 88 (Encl Q23) require commanders to ensure that all personnel assigned to sensitive duties are initially indoctrinated and periodically instructed on the national security implications of their duties and on their

individual responsibilities. Both regulations establish that "security programs shall be established to insure supervisory personnel are familiarized with their special responsibilities in matters pertaining to personnel security with respect to personnel under their supervision." (DoD 5200.2-R, paragraph C9.1.3, 2 Feb 96 as amended by OSD Memo "Personnel Security Investigations and Adjudications, 10 Nov 98 (Encl Q31); AR 380-67, paragraph 9-102, 9 Sep 88 (Encl Q23)).

d. (U//~~FOUO~~) Insider Threat Indicators. Prior to October 2010, AR 381-12 (Encl Q16) covered the topic of Subversion and Espionage Directed Against the Army (SAEDA) and mandated an annual training session on the subject for every Soldier. However, SAEDA never adequately addressed the "insider threat." In October 2010, AR 381-12 was revised to include indicators of the "insider threat" and renamed "Threat Awareness and Reporting Program." Table 3-1 of the regulation, titled "Indicators of Espionage," sets out seven behaviors to be considered. Mental instability or other behavioral health issues are not included in the regulation. AR 381-12, Chapter 3 was also revised to strengthen the requirements to report "threat-related incidents." Specifically, the regulation provides that failure to comply with reporting requirements may result in "punishment under UCMJ, as well as adverse administrative or other adverse action." (AR 381-12, paragraph 3-1(a), 4 Oct 10 (Encl Q16)).

2. (U//~~FOUO~~) Facts Pertaining to PFC Manning's Security Clearance.

a. (U//~~FOUO~~) Application. As previously noted, PFC Manning's MOS was 35F, Intelligence Analyst, an MOS which required a TS Clearance. (DA Pam 611-21). On 26 September 2007, PFC Manning electronically submitted his OPM SF 86, Security Clearance Application via e-QIP. (SF 86, 26 Sep 07 (Encl N1)). This investigation discovered that PFC Manning made three false statements on his SF 86. These false statements took the form of PFC Manning's failure to acknowledge a debt, having been fired from a job, and having received behavioral health care.

b. (U//~~FOUO~~) Single Scope Background Investigation (SSBI). PFC Manning's SSBI was conducted from 10 October 2007 through 15 January 2008 and covered a period of time from September 2005 (PFC Manning's return to the U.S. from the U.K.), through the end of 2007. (JAMS, 28 Dec 10 (Encl N2)). During the SSBI, several issues were noted by the investigator: PFC Manning's mother was a citizen of the U.K. and he had approximately $2,500 in debt ($1472.51 owed to a previous landlord and three other collection accounts totaling $929.00). (SF 86, Investigators Notes (Encl N1)). The investigation does not reveal any follow-up investigation regarding the debt or the fact that PFC Manning failed to answer truthfully all questions on his SF 86. Furthermore, during his personal interview, PFC Manning disclosed that he was fired from a job and that his stepmother had called the police accusing PFC Manning of threatening her. The investigation did not reveal any follow-up on the fact that PFC Manning had indicated on his SF 86 that he had never been fired from a job. In regard to PFC

Manning's statement about his stepmother, the investigator ran a check of police records and found no mention of the alleged assault. (Army G-2 MFR, 28 Jan 11 (Encl O4)). The investigation does not reveal any other follow-up by the investigator (the stepmother was not interviewed). When asked about these issues, personnel from the Federal Investigative Services (OPM) stated that it was determined that there was no need to interview the stepmother because there was no police report. Further, the debt did not exceed the threshold amount ($7,500) that would allow the investigator to initiate an additional contact to confront PFC Manning. (Email Federal Investigative System, 1 Feb 11 (Encl O18)).

c. (U//~~FOUO~~) Adjudication. Once completed, the investigation was forwarded to the Army CCF for adjudication. Both Manning's foreign influence (i.e., mother a UK citizen) and his debt were mitigated in the adjudication phase. His mother's UK citizenship (i.e., "foreign influence") was mitigated because of the nature of the relationship to the foreign citizen (i.e., familial-mother) and the lack of susceptibility to coercion (i.e., a determination that the foreign influence would not make PFC Manning susceptible to coercion due to foreign national conflict). The debt was mitigated because it was determined to be a minor amount below the DoD acceptable debt standard of $7,500. If the total debt is less than the DoD standard, it is not considered in the adjudication process. (Army G-2 MFR, 28 Jan 11 (Encl O4); SF 86, Investigators Notes (Encl N1)). On 6 October 2008, PFC Manning was granted a Top Secret/Sensitive Compartmented Information (TS/SCI) level clearance. (OPM File (Encl N4); JAMS, 28 Dec 10 (Encl N2); Army G-2 Memorandum, 28 Dec 10 (Encl Q-42)).

d. (U//~~FOUO~~) Issues Not Considered During Security Clearance Process. The following are issues that were either not known by the investigators and adjudicators assigned to PFC Manning's case, or known to them, but not fully considered. Each of these issues raises concerns regarding PFC Manning's trustworthiness and reliability.

(1) (U//~~FOUO~~) PFC Manning's Time in the UK. As OPM does not have jurisdiction to conduct background investigations in a foreign country, no one in the UK was interviewed. In a newspaper interview conducted after the Wikileaks incident became public, one of PFC Manning's UK high school classmates described PFC Manning as a "troublemaking, authority-hating, computer geek." (UK Telegraph Article, 29 Jul 10 (Encl O21)).

(2) (U//~~FOUO~~) Pre-Army Behavioral Health Issues. Section 21 of the SF 86 asks: "In the last 7 years, have you consulted with a behavioral health professional (psychiatrist, psychologist, counselor, etc.) or have you consulted with another health care provider about a mental health related condition?" PFC Manning answered this question, "No." The security clearance investigation did not discover any information regarding PFC Manning's previous behavioral health concerns or prescription for behavioral health related drugs, and therefore these issues were not considered during

the security clearance process. Although the Section 21 question was subsequently revised by an 18 April 2008 Secretary of Defense Policy Memorandum, Subject: Policy Implementation - Mental Health Questions, SF 86, Questionnaire for National Security Positions, PFC Manning would have been required to answer the questions truthfully. The 2008 Secretary of Defense policy states an individual can answer "no" to the behavioral health questions if they received counseling or were hospitalized for "strictly marital, family, grief, not related to violence [by the individual]" or "strictly related to adjustments from service in a military combat environment." PFC Manning sought assistance for anxiety issues not related to any military deployment, and therefore the 2008 Secretary of Defense policy would not have excused him from answering Question 21 in the affirmative and disclosing the nature of his previous treatment. (SECDEF Policy, 18 Apr 08 (Encl O24)).

(3) (U//~~FOUO~~) Nature of Debt. From the adjudication process, it appears that the nature of PFC Manning's debt to the Coopermill Apartments was not considered because the amount of debt was less than the DoD acceptable standard of $7500. Rather than satisfying his financial obligations, PFC Manning "skipped out" on the lease by abandoning his apartment without telling the landlord. The manner in which the debt was accrued raise questions about PFC Manning's reliability and trustworthiness that should have been considered during the adjudication process. (SF 86, 4 Oct 07 (Encl N-3)).

(4) (U//~~FOUO~~) Military Incidents. By the time his security clearance was awarded on 6 October 2008, PFC Manning had at least three notable incidents: alleged assault of another Soldier in November 2007; command referral to Behavioral Health in March 2008; and potential security violations while at AIT between April and September 2008. The first incident occurred during the SSBI investigative stage and the latter two during the adjudication phase of PFC Manning's clearance application processing. The OPM investigators (and the command) were unaware of the first incident. As no derogatory reports were forwarded to the CCF (JAMS, 28 Dec 10 (Encl N2)), none of the incidents were considered during the adjudication phase of PFC Manning's security clearance process.

e. (U//~~FOUO~~) Failure to Evaluate Continued Eligibility.

(1) (U//~~FOUO~~) Reporting Requirements. Despite PFC Manning's conduct and behavioral health issues, his supervisors failed to tie or link his actions to his security clearance. Regulations require that derogatory information within the scope of AR 380-67, paragraph 2-200, be immediately forwarded to the commander or security officer. (AR 380-67, paragraph 8-101, 9 Sep 88 (Encl Q23)). Further, commanders are required to immediately forward credible derogatory information to the CCF. (AR 380-67, paragraph 8-101(b)(1), 9 Sep 88 (Encl Q23)).

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

(2) (U//~~FOUO~~) Misconduct within the Scope of AR 380-67, Paragraph 2-200. A review of PFC Manning's conduct since entering active duty indicate that there were no less than fourteen discrete events, occurring on different dates and times, prior to his 25 May 2010 apprehension, which individually, or in the aggregate, should have resulted in a DA Form 5248-R, *Report of Unfavorable Information for Security Determination*, being forwarded to CCF:

1. NOV 2007 - PFC Manning allegedly assaults another Soldier at basic training (*not reported by Soldiers, no action taken*);

2. MAR 2008 - PFC Manning is command referred to Behavioral Health for "tantrum fits of rage" (*no further action, "not abnormal for basic training"*);

3. JUN 2008 - PFC Manning posted videos on YouTube discussing his access to classified information and left computer terminal unsecured. *(Possible UCMJ action, counseling and corrective training; no records available, no DEROG)*;

4. APR 2009 - PFC Manning counseled for failure to repair resulting in an emotional outburst and a self-referral to Behavioral Health (*command not informed by supervisor, no UCMJ or DEROG report*);

5. APR/MAY 2009 - PFC Manning makes statement that he has "no loyalty" to the United States and that the patch (i.e., American Flag) on his shoulder "meant nothing to him" (*command not informed by supervisor, no UCMJ or DEROG report*);

6. APR/MAY 2009 - PFC Manning states to another Soldier that he had erased his internet blogs before he joined the Army or he would not have received a security clearance (*MSG (b) (6) informed; command not informed, no UCMJ or DEROG report*);

7. AUG 2009 - Negative counseling at JRTC for FTR followed by emotional outburst where PFC Manning shoves chair (*command not informed by supervisor, no UCMJ or DEROG report*);

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

8. DEC 2009 - PFC Manning is counseled by MSG (b) (6), for losing his room key and has an emotional outburst; (*command not informed by supervisor, no UCMJ or DEROG report*);

9. DEC 2009 - PFC Manning is counseled for another FTR and has an emotional outburst, is disrespectful and insubordinate and commits an assault on ("assault by offer" in violation of Article 128, UCMJ) SPC (b) (6), in the SCIF (*command referred to Behavioral Health; counseled by 1SG, no further inquiry by commander to determine exactly what happened, no UCMJ action, no DEROG report*);

10. DEC 2009 - PFC Manning sees Behavioral Health Care Provider– report states PFC Manning (b) (6), (b) (7)(C) . PFC Manning is deemed fit for duty. Separation not warranted (unless outbursts continue); however, provider noted PFC Manning was a moderate risk for aggression and recommended that command consider removing the weapon or bolt from his weapon (*no DEROG Report*);

11. FEB/MAR 2010 - Soldiers in SCIF talking about why they joined the Army; PFC Manning said the US flag meant nothing to him and he had no loyalties to the US. CW2 (b) (6), (b) not concerned about PFC Manning's patriotism, but about whether PFC Manning was depressed or had anger issues (*command not informed, no DEROG report*);

12. APR 2010 - PFC Manning sends MSG (b) (6), an Email Subject "My Problem" with an attached photograph of himself in a wig with make-up, portraying himself as a woman (*command not informed, no DEROG report*);

13. MAY 2010 - PFC Manning sends an Email to SGT (b) (6), and SSG (b) (6), (b) with a cc to MSG (b) (6), Subject "Situation" wherein he describes the end of a "close relationship" (*command not informed, no action taken*); and

14. MAY 2010 - PFC Manning physically assaults SPC (b) (6), (b) (command informed by 1LT (b) (not MSG (b) (6), PFC Manning receives non-judicial punishment (Company Grade Article 15) with adjudged reduction

from SPC to PFC and forfeiture of $446 pay for one month, separation initiated (behavioral health evaluation conducted), DEROG filed).

f. (U//~~FOUO~~) Command Awareness. While MSG [redacted] was aware of the great majority of these events, it does not appear that he informed the command about each of these incidents or the full nature of PFC Manning's conduct and behavioral health issues. With the exception of the December 2009 outburst related to SPC [redacted] it appears the chain of command was uninformed of all others. (DA Form 2823, [redacted] 20 Jan 11 (Encl E23-2); DA Form 2823, [redacted] 18 Jan 11 (Encl E82-1); DA Form 2823, [redacted] 20 Jan 11 (Encl E56-1); DA Form 2823, [redacted] 5 Jan 11 (Encl E85-1)). With regards to the December outburst involving SPC [redacted] the command did refer PFC Manning to behavioral health and counsel him (DA Form 2823, [redacted] 18 Jan 11 (Encl E82-1)), however, no action was taken in regard to his security clearance. (JAMS, 28 Dec 10 (Encl N2)). The company commander also failed to conduct any further inquiry to determine the exact nature of the situation. (DA Form 2823, [redacted] 20 Jan 11 (Encl E23-2)).

g. (U//~~FOUO~~) May 2010 Derogatory Information. Only after PFC Manning assaulted SPC [redacted] and received a formal Company Grade Article 15 was a DA Form 5248-R, *Report of Unfavorable Information for Security Determination,* completed. (DEROG, 9 May 11 (Note –erroneously dated in original as 2011, however, actual date was 2010 (Encl N5)). Due to administrative issues in theater, the report was not forwarded to CCF until 18 June 2010. (Army G-2 Memorandum, 28 Dec 10 (Encl Q42); DA Form 2823, [redacted] 20 Jan 11 (Encl E56-1)).

h. (U//~~FOUO~~) Behavioral Health Issues and Security Clearance.

(1) (U//~~FOUO~~) PFC Manning. PFC Manning's behavioral health issues prompted no action related to his security clearance at the 2/10 MTN level until May 2010. Prior to May 2010, PFC Manning's supervisors and those aware of his behavioral health issues believed that PFC Manning might be a threat to himself or others, but never considered him a security threat.

(2) (U//~~FOUO~~) Division Process. According to LTC [redacted], United States Division-Central (USD-C) G-2, command referrals to Behavioral Health for Division-level Soldiers would be reviewed by the G-2 and G-2 SGM for purposes of determining whether a Soldier's clearance should be suspended. There was no such process at 2/10 MTN. Depending on the nature of the situation, a suspension of access may or may not have been followed up by a derogatory report to the CCF. (Interview MFR, [redacted] 24 Jan 11 (Encl E39-1)).

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

Section ID: SCI Physical Security

1. (U//~~FOUO~~) SCI Physical Security and 2/10 MTN SCIF Operations.

a. (U//~~FOUO~~) Applicable Regulations. The following section sets out the applicable regulations in the area of SCI Physical Security.

(1) (U//~~FOUO~~) Intelligence Community (IC) Hierarchy. In the area of physical security for SCIFs, regulatory guidance is provided at the national level. The Director of National Intelligence (DNI) is the head of the United States Government Intelligence Community (IC), having replaced the Director of Central Intelligence (DCI), who held that position until 2005. DNI policies are implemented by the various government agencies through Cognizant Security Authorities (CSAs). The IC CSA for all agencies under the DoD, including the Department of the Army, is the Defense Intelligence Agency (DIA). As the DoD CSA, DIA promulgates the DoD Sensitive Compartmented Information (SCI) physical security policy set by the DNI.

(2) (U//~~FOUO~~) Office of the Director of National Intelligence (ODNI) Policies.

(a) (U//~~FOUO~~) DCID 6/9 (Encl Q25). The Director of Central Intelligence Directive (DCID) 6/9, Physical Security Standards for SCI Facilities, was the DNI policy in place at the time of the that PFC Manning is alleged to have disclosed classified material. DCID 6/9 was published in 2002 under the authority of the DCI. When DNI replaced the DCI as the head of the IC, the DCID 6/9 was adopted as a DNI policy. (Army G-2 Memo, 28 Jan 11 (Encl O4)).

(b) (U//~~FOUO~~) DCID 6/9 Amended 1 December 2005. On 1 December 2005, ODNI published ICP Memorandum No. 2005-700-1, which superseded Annex D, Part I of DCID 6/9. Annex D, Part I pertained to electronic equipment in SCIFs. (ICP Memo 2005-700-1, 1 Dec 05 (Encl Q61)).

(c) (U//~~FOUO~~) DCID 6/9 Rescinded 26 May 2010. On 26 May 2010, Intelligence Community Directive (ICD) Number 705 rescinded DCID 6/9, but provided that "IC elements may continue to operate SCIFs accredited as of the effective date of this Directive in accordance with physical and technical security requirements applicable at time of the most recent accreditation or re-accreditation." (ICD No. 705, Sensitive Compartmented Information Facilities, paragraphs B.2. and D.3., 26 May 10 (Encl Q57)). Further, paragraph D.2. of ICD No. 705 states new guidance will be published within 90 days. (ICD No. 705, paragraph D.2, 26 May 10 (Encl Q57)). According to Department of the Army G-2 personnel, DIA has stated that DCID 6/9 is the standard for all current SCIFs until the ICD policy has been signed. (Email, Schoch, 2 Feb 11 (O29)). ICD No. 705.1 was signed on 17 September 2010; however, it refers to the Technical Specification for Construction and Management of Sensitive Compartmented

Information Facilities, which is still in draft form. (ICD Memorandum Number 705.1, 17 Sep 10 (Encl Q58); Technical Specification for Construction and Management of Sensitive Compartmented Information Facilities, v. 10, January XX, 2011 (draft) (Encl Q60); (Email, (b) (6) 7 Feb 11 (Encl O34)).

(3) (U//~~FOUO~~) DoD 5105.21-M-1 (Encl Q24). DIA's guidance for SCIFs is provided in DoD 5105.21-M-1, often referred to as simply the "M-1" by those in the IC. In a deployed theater, the Combatant Command's Special Security Officer (SSO) also has security cognizance. (DoD 5105.21-M-1, Chapter 1, paragraph D.3, Aug 98 (Encl Q24)). The M-1 predates the DCID 6/9 by four years.

(4) (U//~~FOUO~~) Army Regulations. AR 380-28, Department of the Army Special Security System is classified CONFIDENTIAL and implements DoD 5105.21-M-1 (Encl Q24)). AR 380-28 requires the establishment of an Entry and Exit Inspection Program to deter removal of classified materials from a SCIF without authorization. AR 380-5, Department of the Army Information Security Program (Encl Q11) was published on 29 September 2000 and provides specific guidance for the SCIF Entry Exit Inspection Program and Two Person Integrity for TOP SECRET Information. (AR 380-5, paragraph 6-36, 29 Sep 00 (Encl Q11)). AR 380-5 predates DCID 6/9 by 2 years. An ODCSINT (now Army G-2) Memorandum dated 4 June 2001, states that any conflict between AR 380-28 and the M-1 would be resolved in favor of the policies and standards set out in the M-1. (ODCSINT Memo Re: DOD 5105.21-M-1, 4 Jun 01 (Encl Q43)).

b. (U//~~FOUO~~) Regulatory Requirements.

(1) (U//~~FOUO~~) SCI Physical Security Personnel. DoD and Army Regulations set out the roles and responsibilities of SCI physical security personnel. These include: Senior Intelligence Officer (SIO); Special Security Officer (SSO); and the Special Security Representative (SSR). Figure 5 below captures pictorially the SCI physical security layout during 2/10 MTN's deployment.

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

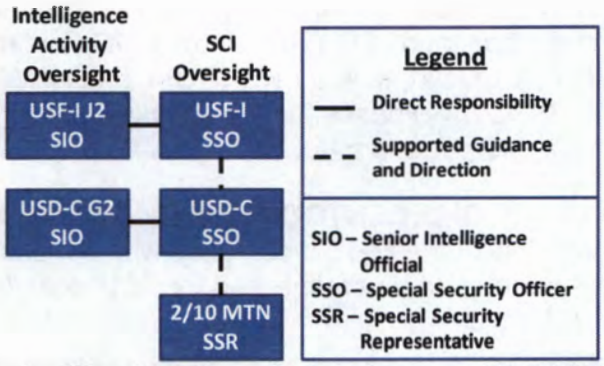

Figure 5: Theater Physical Security Laydown re: 2/10 MTN (U//~~FOUO~~)

(2) (U//~~FOUO~~) Senior Intelligence Officer (SIO). The SIO is the highest ranking person charged with intelligence and security functions within a command or element of an IC organization. (DoD 5105.21-M-1, August 1998, Chapter 1, paragraph F.4, Aug 98 (Encl Q24)). For USF-I the SIO was the J2. For USD-C, the SIO was the Division G-2. According to the M-1, the SIO should be of a rank no lower than O-5 or civilian equivalent grade. (DoD 5105.21-M-1, Chapter 1, paragraph F.4., Aug 98 (Encl Q24)). The SIO exercises overall management of SCI. Among the many functions of the SIO is appointment of Special Security Officers (SSO) and Special Security Representatives (SSR). (DoD 5105.21-M-1, Chapter 1, paragraph F.4.a. Aug 98 (Encl Q24)). When not deployed, all SSRs below division level should be trained and appointed by the G-2 of the division or corps headquarters exercising Training and Readiness Oversight (TRO). As applied to the "modular" Army, SIOs or G-2s of divisions accepting operational control of brigades from other organizations also accept the brigade SSRs that have been trained and appointed by those brigades' senior headquarters at home station. (Interview MFR, (b) (6) 24 Jan 11 (Encl E39-1); USF-I J2 Memorandum, 21 Jan 11, paragraph 5 (Encl Q46)).

(3) (U//~~FOUO~~) Special Security Officer (SSO). The SSO is a commissioned officer, warrant officer or civilian (GS-9 or above). The SSO provides SCI security oversight for SCIFs in the SSO's area of operations. Among other duties, the SSO conducts or otherwise manages SCI personnel, SCI information, physical and technical security actions and physical and technical security procedures. (DoD 5105.21-M-1, Chapter 1, paragraph F.5.a(6), Aug 98 (Encl Q24)).

(4) (U//~~FOUO~~) Special Security Representative (SSR). The SSR, under the direction of the supporting SSO, is responsible for the day-to-day management and implementation of SCI security for a "separate subordinate SCIF." The SSR is a commissioned officer, warrant officer, the most senior non-commissioned officer (of the SCIF) or a civilian in the grade of GS-7 or above. (DoD 5105.21-M-1, Chapter 1, paragraph F.5.b., Aug 98 (Encl Q24)).

(5) (U//~~FOUO~~) T-SCIF[6] Approval Authority. T-SCIF approval authority was delegated to U.S. Central Command (CENTCOM) for T-SCIFs deploying in support of Operations ENDURING FREEDOM, IRAQI FREEDOM, and NEW DAWN. (DA G-2 Memorandum, Subject: T-SCIF Guidance for Army Units Deploying in support of Operation Enduring and IRAQI Freedom (OEF/OIF), 27 Feb 06 (Encl Q53)).

(6) (U//~~FOUO~~) CENTCOM. CENTCOM published guidance on SCI physical security that was consistent with the M-1. It complied with DCID 6/9 with the exception that it did not require procedures to be established for SCIF entry/exit inspections. (CCR 380-12, 4 Aug 10 (Encl Q44)).

(7) (U//~~FOUO~~) USF-I. USF-I published a USF-I J2 SSO Operating Procedures which focused solely on personnel security (USF-I SSO SOP, undated (Encl Q63)). USF-I did not have any SSO/SSR training program in place because units are required to ensure SSOs/SSRs have attended appropriate training prior to arrival in theater (USF-I J2 Memorandum, 21 Jan 11 (Encl Q46)). While USF-I did not mandate formal SSO/SSR training, training and reference materials were available via the USF-I command security website. (USF-I J2 Memorandum, 21 Jan 11 (Encl Q46)).

(8) (U//~~FOUO~~) Policy on Rewriteable Media in a SCIF. Annex D of DCID 6/9, as amended on 1 December 2005 by ICP No. 2005-700-1, sets out the policy on Personal Electronic Devices (PED). The amended Annex D also provides guidance regarding the need to establish mitigation policies for high and medium vulnerability electronic devices. (ICP No. 2005-700-1, 1 Dec 05 (Encl Q61). On 25 August 2006, DIA published the DIA SCIF PED Policy, with an effective date of 1 November 2006. The DIA SCIF PED Policy lists "hardware/software associated with PEDs and removable magnetic/optical media, storage devices, thumb drives, etc" as high-vulnerability PEDS and states that only government owned devices are allowed in SCIFs. (DIA SCIF PED Policy, 25 Aug 06 (Encl Q18)). Annex D was updated in 2005. Further, the Security Safeguard section states ". . . electronic media such as floppy disks, CDs etc . . . Must be closely controlled by the SSO." (DIA SCIF PED Policy, 25 Aug 06 (Encl Q18)).

(9) (U//~~FOUO~~) Entry/Exit Inspection Programs. DCID 6/9 states that the CSA "shall prescribe procedures for inspecting persons, their property, and vehicles at the entry or exit points of SCIFs, or at other designated points of entry to the building, facility, or compound. The purpose of the inspection is to deter the unauthorized removal or classified material, and deter the introduction of prohibited items or contraband. This shall include determination of whether inspections are randomly

[6] (U) The 2/10 MTN Sensitive Compartmented Information Facility was a Tactical SCIF which is properly referred to as a T-SCIF. For purposes of this investigation, the relevant polices are the same for both T-SCIFs and SCIFs, except for the approval process. Because the overwhelming majority of references to the 2/10 MTN Facility is as a SCIF, this report references the 2/10 MTN facility as a SCIF.

conducted or mandatory for all, and whether they apply for visitors only or for the entire staff assigned." (DCID 6/9, 18 Nov 02, paragraph 2.7, 18 Nov 02 (Encl Q25)). The draft ODNI guidance for SCIFs states that SCIF SOPs should address "personnel and package inspection procedures." (Tech Spec, paragraph D.7 (Encl Q60)). DIA's policy as set out in the M-1 does not identify procedures for conducting entry/exit inspections. AR 380-5 states, "[t]he previous edition of this regulation required commands to establish a program to inspect for the unauthorized removal of classified information. Although this program, known as the Entry/Exit Inspection Program is, effective by this regulation, no longer a Department of the Army-wide requirement, it does remain an effective tool that can be used in command security programs to deter and detect the unauthorized removal of classified information." (AR 380-5, paragraph 6-36, 29 Sep 00 (Encl Q11)).

(10) (U//~~FOUO~~) Inspections and Staff Assistance Visits. The M-1 authorizes inspections or staff assistance visits (SAVs) to SCIFs, but does not require inspections or SAVs by higher headquarters after the initial accreditation inspection. "After initial security authorization, approval, certification, or accreditation, inspections will be conducted aperiodic (sic) or random (sic) and will be based on risk management principles." (DoD 5105.21-M-1, Chapter 1, paragraph M.2., Aug 98 (Encl Q24); DCID 6/9, paragraph 2.3.3, 18 Nov 02 (Encl Q25)). The M-1 does require that units conduct a self-inspection at least annually. (DoD 5105.21-M-1, Chapter 1, paragraph M.1, Aug 98. (Encl Q24)).

(11) (U//~~FOUO~~) Training of SCI Physical Security Personnel. The M-1 charges DIA with establishing training for SCI Physical Security Personnel, but does not require attendance by SCI Physical Security Personnel at DIA training. (DoD 5105.21-M-1, Chapter 1, paragraph F.1.g., Aug 98 (Encl Q24)). The SIO has responsibility to ensure SSOs and SSRs receive training to perform their respective duties and responsibilities, but the amount and type of training is not specified. (DoD 5105.21-M-1, Chapter 1, paragraph F.4.h., Aug 98 (Encl Q24)). DIA offers a 64-hour SSO training course (5 day residency with 2 prerequisite on-line courses), but there is no regulatory requirement for SSOs or SSRs to attend. In contrast, the SSR training at Fort Drum consisted only of a one-hour block of instruction covering more than 100 slides. (DA Form 2823, (b) (6), 28 Jan 11 (Encl E17-2); DA Form 2823, (b) (6), 6 Jan 11 (Encl E4-1)).

c. (U//~~FOUO~~) 2/10 MTN SCIF Operations. When 2/10 MTN deployed to Iraq, it fell under the command and control of Multi-National Division-Baghdad (MND-B), 1st Cavalry Division (1CD). In January 2010, 1st Armored Division (1AD) relieved 1CD in place and assumed duties as USD-C, which replaced both MND-B and the former Multi-National Forces-West (MNF-W). (Interview MFR, (b) (6), 24 Jan 11 (Encl E39-1); DA Form 2823, (b) (6), (b) 21 Jan 11 (Encl E27-1)).

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

(1) (U//~~FOUO~~) Accreditation and Oversight of the 2/10 MTN SCIF.

(a) (U//~~FOUO~~) Accreditation. The accreditation of 2/10 MTN's SCIF was in accordance with DoD and CENTCOM policies. (CCR 380-12, 1 Mar 05 (Encl Q50); CCR 380-3, Sensitive Compartmented Information Access, 23 Oct 08 (Encl Q51); CCR 380-1, Information Security Program Regulation, 1 Apr 07 (Encl Q52)). There is no indication that CENTCOM or USF-I failed to enforce accreditation policies. (DA Form 2823, [redacted], 21 Jul 10 (Encl E58-1); Interview MFR, [redacted], 24 Jan 11 (Enclosure E39-1)). The SIOs for CENTCOM and USF-I both have oversight responsibilities for SCI security programs within their organizations and are charged with implementing the applicable SCI policies. (DoD 5105.21-M-1, Chapter 1, paragraph F.4., Aug 98 (Encl Q24)). A review of theater policies showed that SCI policies were properly implemented.

(b) (U//~~FOUO~~) Division Oversight. The Division G-2, as the SIO, exercises overall management of SCI programs within his organization. The Division SSO has responsibility to oversee SCI Security for subordinate SCIFs. Three separate organizations were responsible for oversight of 2/10 MTN SCI Physical Security during the investigative timeframe: 10th MTN DIV before October 2009; 1CD (MND-B) from October 2009 – January 2010; and 1AD (USD-C) from January 2010 – May 2010.

(2) (U//~~FOUO~~) 10th Mountain Division. As the parent division of 2/10 MTN, 10th MTN DIV provided SCI Physical Security training to 1LT [redacted] and SSG [redacted] The SSO for 10th MTN, SSG [redacted] provided a one-hour training block, covering more than 100 slides, to 1LT [redacted] and SSG [redacted] (DA Form 2823, [redacted] 28 Jan 11 (Encl E17-2); Interview MFR, [redacted] 25 Jan 11 (Encl E17-3)). On 2 June 2010, 1LT [redacted] and SSG [redacted] were appointed as SSRs. Their appointment orders were valid both in garrison and in theater. By regulations, SSOs should be commissioned officers, warrant officers or civilian employees GS-9 or above. When questioned as to why SSG [redacted] was appointed as the SSO, Mr. [redacted] the 10th Mountain Division rear-detachment G-2, stated that his section was not manned appropriately. Three years ago, when the division only had 2 SCIFs, there were 4 enlisted Soldiers and 1 major performing security functions. Today 1 captain and 2 enlisted Soldiers have responsibility for 8 SCIFs. (DA Form 2823, [redacted] 7 Jan 11 (Encl E87-1)).

(3) (U//~~FOUO~~) USD-C. 1CD conducted the accreditation inspection. The 2/10 MTN SCIF was accredited in November 2009. 1AD did not conduct any inspections of the 2/10 MTN SCIF. Neither 1CD nor 1AD conducted any training or appointment of SCI Physical Security Personnel, as the training and appointment had been done by 10th Mountain Division. (DA Form 2823, [redacted] 21 Jan 11 (Encl E27-1); Interview MFR, [redacted] 24 Jan 11 (Encl E39-1); Interview MFR, [redacted] 24 Jan 11 (Encl E58-2); Email, [redacted] 7 February 2011 (O41)). This was in line with USF-I's policy that SCI physical security personnel be trained prior to deployment. (USF-I J2 Memorandum, 21

Jan 11 Encl Q46)). The 1AD SSO stated that 1AD did not provide specific policies for brigades because "no BDE policies are needed since all guidelines are given in the DCID 6/9, (AR) 380-5, and the DoD 5105.21-M-1 and other security manuals." Further, the 1AD SSO stated that no inspections were conducted because "we do not have the manpower to go to these sites and randomly inspect T-SCIFs." (Interview MFR, [redacted] 24 Jan 11 (Encl E58-2)). Given the regulatory responsibilities of the SIO and SSO, inspections or SAVs of brigade SCIFs by Division SIOs and/or SSOs would be one way to enforce established SCI physical security policies.

(a) (U//~~FOUO~~) Self-Inspections. The M-1 required units to conduct self-inspections at least annually. (DoD 5105.21-M-1, paragraph M(1), Aug 98 (Encl Q24)). There was no documentation of a self-inspection conducted by 2/10 MTN. (USF-I J2 Memorandum, 21 Jan 11 (Encl Q46)). However, the requirement is for annual self-inspections, and given the fact that 2/10 MTN's rotation in theater was less than 12 months in duration, 2/10 MTN was not in violation of the policy.

(b) (U//~~FOUO~~) 2/10 MTN SSR. The designated Special Security Representative (SSR) for the SCIF was 1LT [redacted] who was trained by the 10th MTN DIV SSO at Fort Drum. (DA Form 2823, [redacted] 6 Jan 11 (Encl E4-1); DA Form 2823, [redacted] 18 Jan 11 (Encl E28-2); SSO Training Certificate – 1LT [redacted] May 09 (Encl O20)). As the SSR, 1LT [redacted] was responsible for the day-to-day management and implementation of SCI security for a SCIF that was located apart from, and with little oversight by, the higher headquarters. Therefore, she needed to be prepared to fulfill many of the responsibilities of the SSO. In contrast to the DIA's 64 hour long physical security course, her training was one hour in duration and consisted of a classroom lecture covering more than 100 PowerPoint slides. (DA Form 2823, [redacted] 6 Jan 11 (Encl E4-1); DA Form 2823, [redacted] 18 Jan 11 (Encl E28-2); SSR Training Slides (Encl O16)).

(4) (U//~~FOUO~~) Other SSRs. Both 1LT [redacted] and SSG [redacted] were on orders as SSRs, however, SSG [redacted] was not performing duties in the SCIF. (Interview MFR, [redacted] 26 Jan 11 (Encl E57-3)). According to 1LT [redacted] MSG [redacted] assumed the physical security responsibilities of the SCIF, while she was primarily responsible for the personnel security (i.e., verification of visitor's security clearance). MSG [redacted] also states "1LT [redacted] and I shared SCIF accreditation and admin duties." (DA Form 2823 [redacted] 15 Jul 10 (Encl E1-5)). This assertion is supported to an extent by MAJ [redacted] who stated that MSG [redacted] took an active role in the physical security of the SCIF. However, MAJ [redacted] stated that 1LT [redacted] not MSG [redacted] was the SSR. (Interview MFR, [redacted] 19 Jan 10 (Encl E15-1); DA Form 2823, [redacted] 18 Jan 11 (Encl E28-2)). By all accounts, the physical security of the SCIF as it pertained to "outsiders" (i.e., personnel without proper clearances), was conducted in accordance with applicable policies. (DA Form 2823, [redacted] 5 Jan 11 (E85-1); DA Form, [redacted] 6 Jan 11 (Encl E20-1)). This AR 15-6 Investigation failed to uncover any evidence that any unauthorized personnel gained access to the SCIF or were present in

the SCIF unescorted. However, few to no SCI physical security measures were implemented with regard to SCIF personnel with authorized access.

(5) (U//~~FOUO~~) Physical Security Layout. The layout of the SCIF was generally unremarkable. Figure 6 below is a drawing (not to scale) of the 2/10 MTN SCIF.

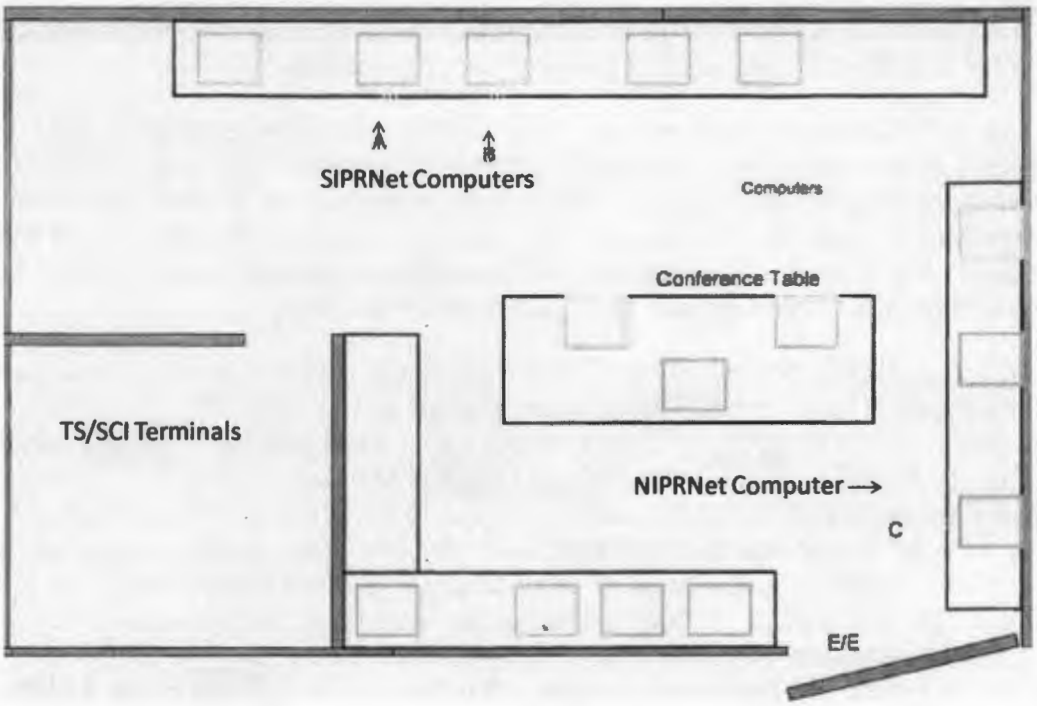

Figure 6: SCIF, Room 14B, 2/10 MTN HQ, FOB Hammer, Iraq (U//~~FOUO~~)

(a) (U//~~FOUO~~) Entry/Exit. The entrance was secured by a cipher lock door and only personnel with authorized clearances were allowed into the SCIF unescorted. When personnel without proper security clearance or access had reason to be in the SCIF, SCIF personnel followed the proper procedures to sanitize the area to the appropriate level of clearance. (Encl O22).

(b) (U//~~FOUO~~) TS/SCI portion of SCIF. The portion of the SCIF where SCI was handled was separated from the collateral[7] side by a server room and a curtain hung in the doorway. Additionally, the computers with access to SCI information were all turned away from the doorway to preclude anyone from seeing the monitors if they entered the

[7] (U) The term "collateral" refers to any classified national security information not otherwise restricted by program or a compartment. The level of classification is distinct from whether that information is collateral or not; not all SCI is necessarily TS.

room. There is no evidence that PFC Manning accessed any information from a SCI computer terminal. (USF-I 15-6 investigation (Encl R1); DA Form 2823, [redacted] 15 Jul 10 (Encl E1-9); DA Form 2823, [redacted] 14 Jun 10 (Encl E47-2); AIR, [redacted] 20 Oct 10 (Encl E31-1); AIR, [redacted] 5 Oct 10 (Encl E62-1)).

(c) (U//~~FOUO~~) Rewritable Media. Rewritable Media were allowed in the SCIF for mission purposes only. Rewritable Media were necessary in order to transfer information from networked SIPRNet computers within the SCIF to interpreters who had security clearances and an official requirement for the information and who worked on stand-alone classified computers, and to share appropriate information with Iraqi counterparts. (DA Form 2823, [redacted] 6 Jan 11 (Encl E46-1); DA Form 2823, [redacted] 20 Jan 11 (Encl E26-3); DA Form 2823, [redacted] 10 Jun 10 (Encl E1-5)). The placement of rewritable media into or on a SIPRNet computer, however, should have resulted in the media itself being labeled as classified and treated as such. (AR 25-2, paragraph 4-17, 24 Oct 07 (Encl Q3)). However, Soldiers who worked in the SCIF were allowed to bring personal music CDs into the SCIF in violation of the DIA SCIF PED Policy. (DIA SCIF PED Policy, 26 Aug 06 (Encl Q18); (DA Form 2823, [redacted] 20 Jan 11 (Encl E26-3); DA Form 2823, [redacted] 10 Jun 10 (Encl E1-5)). According to CW2 [redacted] the majority of CDs brought into the SCIF were factory music CDs which were non-rewritable media. When interviewed, CW2 [redacted] stated that some inspections were conducted to ensure that Soldiers did not have personal rewritable media in the SCIF. (DA Form 2823, [redacted] 20 Jan 11 (Encl E26-3)). However, no other witness corroborates this statement. (DA Form 2823, [redacted] 21 Jan 11 (Encl E65-1); DA Form 2823, [redacted] 7 Jan 11 (Encl E44-2); DA Form 2823, [redacted] 6 Jan 11 (Encl E46-1); DA Form 2823, [redacted] 10 Jun 10 (Encl E1-5)). At the Division SCIF, personnel were not allowed to listen to music or watch movies on the SCIF computers. Any personnel seen wearing headphones were questioned. (Interview MFR, [redacted] 24 Jan 11 (Encl E39-1)).

d. (U//~~FOUO~~) Compromise of Physical Security by PFC Manning. Based on the evidence available to this investigation, particularly PFC Manning's excerpted Internet Relay Chat logs with hacker Adrian Lamo, PFC Manning allegedly downloaded classified information onto his SIPRNet computer, removed that information from his workplace and transferred that information to persons not entitled to receive classified information.

e. (U//~~FOUO~~) According to chat logs PFC Manning noted that: "people stopped caring after 3 weeks;" "there was no physical security;" "it was a massive data spillage . . . facilitated by numerous factors . . . both physically, technically, and culturally . . . perfect example of how not to do INFOSEC;" "[I] listened and lip-synched to Lady Gaga's 'Telephone' while exfiltrating possibly the largest data spillage in American history." He also made the following observations: "weak servers, weak logging, weak physical security, weak counterintelligence, inattentive signal analysis." (USF-I AR 15-6

(Encl R1)). PFC Manning referred to the circumstances in the SCIF as "a perfect storm." (USF-I AR 15-6 (Encl R1)).

2. (U//~~FOUO~~) Comprehensive Security Resiliency Concept. During this investigation, the investigative team was briefed on the Army G-2's "Comprehensive Security Resiliency" concept. As explained to the team, the Army G-2's current "Comprehensive Security Resiliency" concept aligns the DA Personnel Security, Counterintelligence, and Security Education Training and Awareness Program in a comprehensive program that will address program shortfalls and ensure a Security Resiliency Posture in the U.S. Army. "Comprehensive Security Resiliency" is relevant to this investigation and the shortfalls it identifies. Key elements of "comprehensive security resiliency" include: leveraging the personnel security program authorities, which establish a model for Soldier standards and accountability; security education, training, and awareness programs; leveraging automation and technology to implement a continuous evaluation, monitoring, identification and reporting of security and counterintelligence concerns; and use or implementation of a security risk rating tool to aid commanders and others in security decisions. (Army G-2 MFR, 28 Jan 11 (Encl O4)).

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

Section IE: Behavioral Health

1. (U//~~FOUO~~) Command vs. Self-Referral to Behavioral Health. A Soldier can receive a behavioral health evaluation or treatment in one of two ways: 1) the Soldier refers him or herself to Behavioral Health (also referred to as Community Behavioral Health or Combat Stress Clinic (CSC)); or 2) the Soldier is directed to Behavioral Health by his commander. The former is commonly referred to as "self-referred" evaluation or "self-referral" and the latter as a "command directed" evaluation. (DoDD 6490.1 *Mental Health Evaluations of members of the Armed Forces*, 1 Oct 97 (Encl Q36); MEDCOM Reg 40-38 (Encl Q35), "Command Directed Mental Health Evaluations," revised 1 September 2001: MEDCOM CJA Info Paper, 15 Sep 10 (Encl O17)). The term "behavioral health" is the same as, and may be used interchangeably with "mental health."

a. (U//~~FOUO~~) Triggers for Referrals. In the case of a self-referral, a Soldier makes an appointment with his behavioral health care provider and the information exchanged between the Soldier and provider is, in most instances, confidential (i.e., Protected Health Information or PHI). In the case of a command-directed behavioral health referral, the Solder's chain of command directs the Soldier to see Behavioral Health. The command-directed evaluation can be based on a concern for the Soldier's well-being; a concern related to the good order and discipline of the unit; or because another regulation or directive mandates a behavioral health evaluation. An example of the latter is AR 635-200, the administrative elimination (separation) regulation applicable to enlisted personnel. AR 635-200 directs the conduct of a behavioral health evaluation prior to the initiation of particular types of separation actions—the decision to direct a behavioral health evaluation is non-discretionary on the part of the command. (DoDD 6490.1, 1 Oct 97 (Encl Q36); DoDI 6490.4, *Requirements for Mental Evaluations*, 28 Aug 97 (Encl Q37); MEDCOM Reg 40-38, *Commander-Directed Mental Health Evaluations*, 1 Jun 99 (Encl Q35); DoD 6025.18-R, January 2003 (Encl Q38); AR 635-200, *Active Duty Enlisted Administrative Separations,* 6 Jun 2005 (Encl Q27)).

b. (U//~~FOUO~~) Behavioral Health Care Providers and Confidentiality. As a general rule, communications between a Soldier and a behavioral health care provider during a self-referred visit are confidential (i.e., PHI). (MEDCOM Info Paper, HIPAA and Commander's Access to Soldier's Protected Health Information, 15 Sep 10 (Encl O17)).

(1) (U//~~FOUO~~) Self-Referral. The rule of confidentiality applies to self-referral in most situations. However, there are seven exceptions to this confidentiality policy set forth in Undersecretary of Defense Directive Type Memorandum 09-006, July 2, 2009 (DTM 09-006) (Encl Q39). DTM 09-006 states that in cases of self-referral, a health care provider shall . . . [n]otify a commander when a member presents with a behavioral health condition in [the following] circumstances:

(2) (U//~~FOUO~~) Harm to Self. The provider believes there is a serious risk of self-harm by the member.

(3) (U//~~FOUO~~) Harm to Others. The provider believes there is a serious risk of harm to others. This includes any disclosures concerning child abuse or domestic violence consistent with DoDI 6400.06 (Encl Q40).

(4) (U//~~FOUO~~) Harm to Mission. The provider believes there is a serious risk of harm to a specific military operational mission. Such risks may include disorders that significantly impact impulsivity, insight and judgment.

(5) (U//~~FOUO~~) Special Personnel. The member is in the Personnel Reliability Program (DoDI 5210.42 (Encl Q41)) or is in a position that has been pre-identified by Service regulation or the command as having mission responsibilities of such potential sensitivity or urgency that normal notification standards would significantly risk mission accomplishment.

(6) (U//~~FOUO~~) Inpatient Care. The member is admitted or discharged from any inpatient behavioral health or substance abuse treatment facility.

(7) (U//~~FOUO~~) Acute Medical Conditions Interfering With Duty. The member is experiencing an acute behavioral health condition or acute medical regimen that impairs the member's ability to perform his or her duties.

(8) (U//~~FOUO~~) Substance Abuse Treatment Program. The member has entered into a formal outpatient or inpatient treatment program consistent with DoDI 1010.6 for the treatment of substance abuse or dependence. Those who seek alcohol-use education, who have not had an alcohol referral incident (such as arrest for driving under the influence) do not require command notification unless they also choose to be formally evaluated and are diagnosed with a substance abuse or dependence disorder.

(9) (U//~~FOUO~~) Command-Directed Behavioral Health Evaluation. In the case of a command-directed behavioral health evaluation, a commander can request that the behavioral health care provider address specific concerns about and observations of a Soldier by describing those concerns and observations as part of the process that occurs before the provider sees the Soldier (MEDCOM Reg 40-38, *Commander-Directed Behavioral Health Evaluations*, 1 Jun 99 (Encl Q35)). After evaluating the Soldier, a behavioral health care provider gives the chain of command the Soldier's prognosis, diagnosis and the provider's recommendations for the Soldier, recording these elements of information on DA Form 3822. (AR 40-66, paragraph a(3)(c), 4 Jan 10 (Encl Q 64)). However, recall that CPT [redacted] evaluated PFC Manning using "MEDCOM Form 4038." (DA Form 2823, [redacted] 18 Jan 11 (Encl E17-2). Although "MEDCOM Form 4038" provides a detailed evaluation of the Soldier, MEDCOM never

formally approved this form for official use throughout the Behavioral Health community (MEDCOM Email from Ms. [redacted], 21 Jan 11 (Encl O43)). Unlike the "MEDCOM Form 4038," the DA Form 3822 contains no reference whatsoever to the suitability of the Soldier for continued access to classified information. Because "MEDCOM Form 4038" remains an informally generated, unapproved form and it has never been generated in a fillable format, behavioral health care providers can delete blocks and the accompanying information at their discretion. Note that I did not attempt to determine the extent to which the "MEDCOM 4038" is currently being used in the field—clearly it was used by the behavioral health care providers who treated PFC Manning, however.

(10) (U//~~FOUO~~) In the case of a command-directed Behavioral Health evaluation, the chain of command must ask the provider specifically to opine on the security clearance of the Soldier in question; otherwise, the behavioral health care provider is not obligated to advise the chain of command on that issue. Some examples of questions commands may pose include:

(a) (U//~~FOUO~~) Does the Soldier have a behavioral health condition that is contributing to current difficulty?

(b) (U//~~FOUO~~) What is the potential for the Soldier to return to full functioning given successful treatment?

(c) (U//~~FOUO~~) Is the Soldier suitable for carrying a weapon at the current time?

(d) (U//~~FOUO~~) Is it appropriate for the Soldier to have access to classified information?

(e) (U//~~FOUO~~) Is the Soldier qualified for deployment?

2. (U//~~FOUO~~) Behavioral Health Issues and Security Clearances. A review of the references cited in DTM 09-006, as well as other regulations, policies and information papers related to behavioral health evaluations and treatment reveals that only one source addresses access to classified information, DoDD 5210.42. (DoDD 5210.42, June 2006 Incorporating Change 1, (10 Nov 09), Nuclear Weapons Personnel Reliability Program (PRP), paragraph. 3.7. (Encl Q41)). That said, this Directive's discussion of classified information occurs in the context of requiring a clearance to perform nuclear weapons duties, and fails to otherwise address the relationship between the findings of a behavioral health evaluation and the award of, or continued access to, a clearance. (DoDD 5210.42, paragraph 3.7. (Encl Q41)).

a. (U//~~FOUO~~) Review of Regulations and Policy. The statutes, Code of Federal Regulations (CFR), Directives, Instructions, Regulations and policies applicable to

determining the nature and quantity of information that may be disclosed to the chain of command by a behavioral health care provider at the conclusion of a Soldier's behavioral health evaluation are consistent in one respect – they are silent on the issue of a Soldier's access to classified information after undergoing a behavioral health evaluation, whether self- referred or command-directed. Beyond a limited discussion of classified material in DoDD 5210.42, none of the references reviewed by this investigative team and cited in the footnote below, establish a requirement for a behavioral health care provider to assess, or, in the alternative to recommend that the chain of command assess, whether the Soldier undergoing evaluation should be permitted to access classified information.[8]

b. (U//~~FOUO~~) Serious Risk.

(1) (U//~~FOUO~~) With regard to self-referrals for behavioral health evaluation, the provisions of DTM 09-006 (Q-39), Attachment 2, focus on whether the Soldier is a serious risk to self, others or the mission, with the degree of mission risk being a discretionary call on the part of the provider. Also of note is that the risk posed by the Soldier to self, others or the mission must be "serious" to warrant reporting to the Soldier's chain of command. Thus, only when the behavioral health care provider deems the risk posed by the Soldier to be "serious" will the command be informed and afforded the option under AR 380-5 to suspend the Soldier's access to classified information and to determine whether a derogatory report should be forwarded to CCF for a determination of whether the Soldier remains suitable for access to classified information.

(2) (U//~~FOUO~~) Behavioral Health Care Provider Report to Command. When a provider believes the Soldier presents a "serious" risk, the provider reports that finding to the command. The command, not the provider, has the authority to take action to

[8] (U) These references include Title 10, United States Code, § 1034 (Protected communications; prohibition of retaliatory personnel actions); Public Law 102-484 (HR 5006), National Defense Authorization for Fiscal Year 1993, October 23, 1992; DoD 6025.18-R, *DoD Health Information Privacy Regulation*, January 2003; DoDI 1010.6, *Rehabilitation and Referral Services for Alcohol and Drug Abusers*, March 13, 1985; DoDI 6025.18, *Privacy of Individually Identifiable Health Information in DoD Health Care Programs*, December 2, 2009; DoDI 6400.06, *Domestic Abuse Involving DoD Military and Certain Affiliated Personnel* August 21, 2007; DoDI 6490.1, *Mental Health Evaluations of Members of the Armed Forces*, 1 Oct 1997; DoDI 6490.4, *Requirements for Mental Health Evaluations of Members of the Armed Forces*, 28 Aug 1997; Directive-Type Memorandum (DTM) 09-006, *Revising Command Notification Requirements to Dispel Stigma in Providing Mental Health Care to Military Personnel*, July 2, 2009; AR 40-66, *Medical Record Administration and Health Care Documentation*, 17 June 2008; MEDCOM Regulation No. 40-38, *Command Directed Mental Health Evaluations*, September 2001; OTSG/MEDCOM Policy Memorandum 10-042, *Release of Protected Health Information (PHI) to Unit Command Officials*, 30 June 2010; and MEDCOM CJA Information Paper, *HIPAA and Commander's Access to Soldier's Protected Health Information*, 15 September 2010.

suspend, or initiate action to revoke, a Soldier's security clearance whenever it perceives the Soldier might compromise security. This broad standard gives a command significant leeway in terms of when and under what circumstances it is permitted to suspend a Soldier's access to classified information. DoD 6025.18-R allows for the release of PHI to "[c]ommanders who exercise authority over an individual who is a member of the Armed Forces, or other person designated by such a commander . . . in order to carry out an activity under the authority of the commander." (DoD 6025.18-R, paragraph C7.11.1.2.1., Jan 03 (Encl Q38)). Because commanders are responsible for taking action to suspend a Soldier's access to classified information or to submit DEROGs to CCF in certain circumstances, they should be given relevant information from providers that address a Soldier's "fitness for duty," "fitness to perform any particular mission," and "fitness to carry out any other activity necessary to the proper execution of the mission of the Armed Forces." DoD 6025.18-R, paragraph C7.11.1.3., January 2003 (Encl Q38)).

3. (U//~~FOUO~~) PFC Manning's Behavioral Health. A review of PFC Manning's Medical and Behavioral Health records and three comprehensive MFRs authored by the S-2 NCOIC, MSG (b) (6), (b) (7)(C) documenting PFC Manning's behavioral health issues over the period from 28 March 2008 through 28 May 2010, reveal multiple behavioral health-related events. PFC Manning's additional consultations with behavioral health care providers subsequent to his apprehension are not addressed in this report for several reasons: (1) they were initiated primarily to determine how PFC Manning was handling incarceration and his risk of suicide; and (2) these assessments have no relevance to the alleged compromise of classified information because PFC Manning had neither access to nor the ability to disclose classified information after his 27 May 2010 apprehension.

a. (U//~~FOUO~~) Sequence of Events. An enumeration of PFC Manning's behavioral health related events/consultations in the 26 months preceding his apprehension follows:

28 March 2008 – Command-Referred (Tantrum and Fits of Rage), FLW.

30 June 2009 – ~~Self-Referred~~ at urging of NCOIC. Diagnosed with (b) (6), (b) (7)(C) released without limitations . . . follow up as needed." (30 Jun 09 SF 600 (Encl M1-2)), Fort Drum.

19 August 2009 – ~~Self-Referred~~ for ("Losing Bearing" and "Going Down Hill"). (b) (6), (b) (7)(C) released without limitations . . . (b) (6), (b) (7)(C) (SF 600, 19 Aug 09 (Encl M1-3)), Fort Drum.

15 September 2009 – ~~Self-Referred~~ (Difficulty doing what he is supposed to do); (b) (6), (b) (7)(C)

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

(b) (6), (b) (7)(C) released without limitations." (SF 600, 15 Sep 09 (Encl M1-4)), Fort Drum.

23 September 2009 – States Command-Referral but appears to be Self- Referral based on advice of someone in chain of command; (b) (6), (b) (7)(C) released without limitations." (SF 600, 23 Sep 09 (Encl M1-5)), Fort Drum.

29 September 2009 – Self-Referred (Follow Up); (b) (6), (b) (7)(C) Released without limitations . . . Provider Comment: "He is doing fine." (SF 600, 29 Sep 09 (Encl M1-6)), Fort Drum.

21 December 2009 – NCOIC (MSG (b) (7) MFR highlighting behavioral health issues (b) (6) Prepared MFR, 21 Dec 09 (Encl E1-1)), Iraq.

24 December 2009 – Command-Referred (Table Flipping Incident in SCIF). (b) (6), (b) (7)(C) Released without limitations . . (b) (6), (b) (7)(C) F 600, 24 Dec 09 (Encl M1-8)), Iraq.

25 December 2009 – Command-Referred. "MEDCOM Form 4038" for bove incident noted PFC Manning was (b) (6), (b) (7)(C) Block 7 – Unsuitability for Access to Classified Information / Clearance (Unchecked), (MEDCOM Form 4038, 25 Dec 09 (M1-1); (b) (6) Prepared MFR, 21 Dec 09 (Encl E1-1)), Iraq.

30 December 2009 – Follow Up (Following Prior SCIF Incident). (b) (6), (b) (7)(C) Released without limitations. (SF 600, 30 Dec 09 (Encl M1-10)), Iraq.

6 January 2010 – "Referral from Previous provider." (Continued Peer Issues). (b) (6) Released without limitations. (SF 600, 6 Jan 10 (Encl M1-11)), Iraq.

16 February 2010 – Scheduled follow up (Continued Difficulty Relating to people). (b) (6), (b) (7)(C) . Released without limitations (SF 600, 16 Feb 10 (Encl M1-12)), Iraq.

2 March 2010 – Scheduled follow up (Continued Treatment). (b) (6), (b) (7)(C) . Released without limitations. (SF 600, 2 Mar 10 (Encl M1-13)), Iraq.

16 March 2010 – Scheduled follow up (Continued Workplace Issues). (b) (6), (b) (7)(C) Released without limitations. (SF 600, 16 Mar 10 (Encl M1-14)), Iraq.

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

23 March 2010 – Scheduled follow up (Continued Workplace Issues). [redacted]. Released without limitations. (SF 600, 23 Mar 10 (Encl M1-15)), Iraq.

30 March 2010 – Scheduled follow up (Continued Workplace Issues). [redacted] Released without limitations. (SF 600, 30 Mar 10 (Encl M1-16)), Iraq.

6 April 2010 – Scheduled follow up (Continued Workplace Issues). [redacted] Released without limitations. (SF 600, 6 Apr 10 (Encl M1-17), Iraq.

26 April 2010 – NCOIC (MSG [redacted] MFR highlighting continued behavioral health concerns. [redacted] prepared MFR, 26 Apr 10 (Encl E1-2)), Iraq.

7 May 2010 – Scheduled follow up (Dismay over "Current Situation"). [redacted] Released with Work/Duty Limitations. (May be a misprint as the date of this appointment was 7 May 10. PFC Manning assaulted SPC [redacted] on the night of 7-8 May and Dr. [redacted] authored these notes on 12 May 10). (SF 600, 7 May 10 (Encl M1-20)), Iraq.

8 May 2010 – Assault on SPC [redacted] in SCIF, Iraq.

8 May 2010 – NCOIC (MSG [redacted] MFR highlighting continued behavioral health concerns. [redacted] prepared MFR, 8 May 10 (Encl E1-3)), Iraq.

8 May 2010 – (Assault on SPC [redacted] "NCOIC brought him in at 0130 because SM had struck another SM in the jaw." [redacted] SM will remain on unit watch until such time as this clinic releases him. Released with work/duty limitations. (SF 600, 8 May 10 (Encl M1-20)), Iraq.

10 May 2010 – Scheduled follow up (Post Assault Therapy, PFC Manning now in Supply). [redacted] Released with work/duty limitations. (SF 600, 10 May 10 (Encl M1-21)), Iraq.

12 May 2010 – Scheduled follow up (40 Minutes Late to Appointment, rescheduled). (SF 600, 12 May 10 (Encl M1-22)), Iraq.

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

13 May 2010 – Scheduled follow up (Anxiety about "Future" in the Army and "Recent Revelations"). (b) (6), (b) (7)(C) [redacted] Released with work/duty limitations. (SF 600, 12 May 10 (Encl M1-23)), Iraq.

15 May 2010 – Scheduled follow up (Anxiety about "Future" in the Army). (b) (6), (b) (7)(C) [redacted] Released with work/duty limitations. (SF 600, 15 May 10 (Encl M1-24)), Iraq.

19 May 2010 – Scheduled follow up (Late to Appointment / Re-Scheduled). (SF 600, 19 May 10 (Encl M1-25)), Iraq.

22 May 2010 – Command-Referred (Assault on SPC (b) (7)(C) [redacted] "MEDCOM Form 4038" noted PFC Manning was (b) (6), (b) (7)(C) [redacted] Block 7 – Unsuitability for Access to Classified Information / Clearance (Deleted). CPT (b) (6), (b) (7)(C) removed block 7 from the Word File of the "MEDCOM Form 4038" because he thought the issue of PFC Manning's access to secret materials was "moot" because PFC Manning was restricted from the SCIF. (b) (6), (b) (7)(C) [redacted] MFR, 25 Jan 11 (Encl E17-3), SF 600, 22 May 10 (Encl M1-26)). Recommended PFC Manning be chaptered out under provisions of AR 635-200, paragraph 5-17, Behavioral Disorder. Released with work/duty limitations. Iraq.

26 May 2010 – Scheduled follow up (Post Article 15-Reduction Visit. Discussing Pending Separation from the Army). (b) (6), (b) (7)(C) [redacted] Released without limitations. (SF 600, 26 May 10 (Encl M1-28)), Iraq.

28 May 2010 – Scheduled follow up. (SF 600, 28 May 10 (Encl M1-29)), Iraq.

28 May 2010 – Command-Referred ("MEDCOM Form 4038"). Deemed a potential high risk of harm to self or others and No longer Suitable for Access to Classified Information / Clearance. ("MEDCOM Form 4038", 28 May 10, SF 600, 28 May 10 (Encl M1-29)), Iraq.

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

b. (U//~~FOUO~~) "MEDCOM Form 4038" (Encl Q26). As stated above, the DA Form 3822, *Report of Mental Status Evaluation*, is the official DA Form approved for use by behavioral health care providers. "MEDCOM Form 4038" was developed a few years ago at Tripler Army Medical Center, Hawaii and was used locally. (MEDCOM Email from Ms. (b) (6), (b) (7)(C) , 21 Jan 11 (Encl O43)). Of the above listed behavioral health-related events, only three were documented in a completed "MEDCOM Form 4038." Of the three "MEDCOM Forms 4038," only the last in time, completed on 28 May 2010, following PFC Manning's assault on SPC (b) (7)(C) noted that PFC Manning lacked suitability for continued access to classified information and that he should not have a clearance.

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

SECTION II: Regulations, Policies and Facts Pertaining to Information Assurance

1. (U//~~FOUO~~) Information Network Background. The Wikileaks incident prompting this AR 15-6 Investigation occurred within the Iraq Joint Operating Area (IJOA), and in the U.S. Central Command (CENTCOM) Area of Responsibility (AOR). Pursuant to the provisions of CENTCOM Regulation (CCR) 25-206, paragraph 2-3, networks in the IJOA were under the command authority of Commander, CENTCOM. CENTCOM delegated the operation and maintenance of the IJOA network to USF-I and its subordinate organizations. (CCR 25-206, chapter 2, paragraph 2-3.a., undated (Encl Q2)).

2. (U) Information Assurance Personnel.

a. (U//~~FOUO~~) Supervisory authority for the network flowed along command lines from CENTCOM to USF-I to USD-C to 2/10 MTN. Supervisory responsibilities for information assurance (IA) vary at each echelon of command, but generally include at least a Designated Approval (or Accreditation) Authority (DAA)[9] and an Information Assurance Manager (IAM). IA duties may be performed as primary or additional duties by a DoD employee (civilian, including local nationals, or military) or by a support contractor. All duty positions have both preparatory and sustaining DoD IA training and certification requirements. Figure 7 shows the echelons of the information assurance workforce from the CENTCOM down to 2/10 MTN

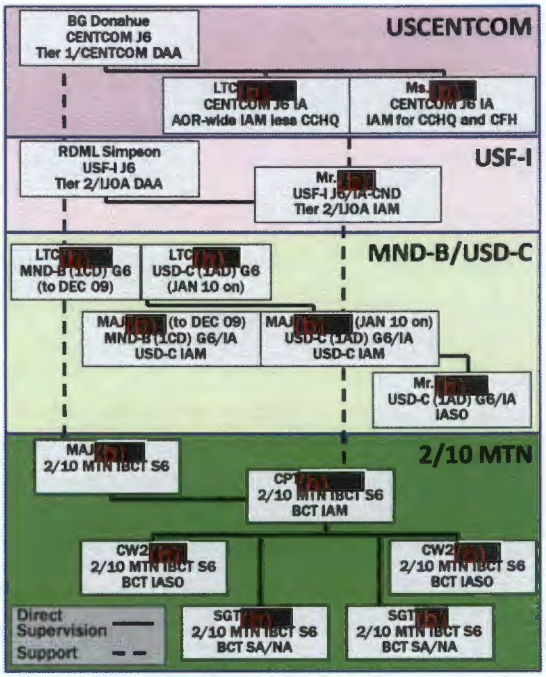

Figure 7. IA Echelons (U//~~FOUO~~)

b. (U//~~FOUO~~) Designated Accrediting Authority (DAA). DoD requires that a DAA be a U.S. citizen, a DoD employee, and have a level of authority commensurate with accepting, in writing, the risk of operating DoD information systems (IS) under his or her purview. (DoDD 8500.01E, paragraph 4.25, 24 Oct 02 (Encl Q1)). CENTCOM prescribes a minimum grade for the DAA as at least O-6/GS-15, and similarly requires vesting the DAA with a level of authority commensurate with accepting, in writing, the risk of operating all IS under their

[9] (U) The terms Designated Accreditation Authority is replacing Designated Approval Authority in practice.

jurisdiction. (CCR 25-206, chapter 7, paragraph 7-5, undated (Encl Q2)). The Army further requires that a DAA be a General Officer, member of the Senior Executive Service, or an equivalent level, regardless of the confidentiality level at which the IS operates. The Army prohibits further delegation of this appointment or downward appointment of DAAs except as set forth in AR 25-2 or as approved by the Army CIO/G–6. (AR 25-2, chapter 5, paragraph 5-8.h., 24 Oct 07 (Encl Q2)). In other words, DAA signature authority must remain in the person appointed as the DAA by the CIO/G-6. Prior to performing the duties of DAA, the designated individual must complete DAA Basics Computer Based Training; meet the training and certification requirements established in National Security Telecommunications and IS Security Committee Instruction (NSTISSI) 4012, *National Training Standard for DAA*, dated August 1997; and be appointed, by name, as DAA by the Army CIO/G–6. (AR 25-2, chapter 3, .paragraph 3-3(m), 24 Oct 07 (Encl Q2)).

(1) (U//~~FOUO~~) The CENTCOM J6 director, BG Brian Donahue, is the DAA for the Tier 1 (theater) architecture in the CENTCOM AOR, and has authorities for all IS in the AOR, except for the Intelligence Community (IC) or to Combat Support Agencies. (CCR 25-206, chapter 2, paragraph 2-5(a), undated (Encl Q2)).

(2) (U//~~FOUO~~) The USF-I Deputy Chief of Staff, Chief of Information Systems (DCS CIS) is the DAA for the IJOA. (MNF-I Directive 25-1, paragraph 6.1., undated (Encl Q4)). The MNF-I staff renamed the DCS CIS as the DCS, CJ6, who at the time of the incident was Rear Admiral (Lower Half) (RDML) David Simpson. (DA Form 2823, (b) (6), , 24 Jan 11 (Encl E91-1)). The USF-I DAA had responsibilities similar to that of his counterpart at CENTCOM, and exercised DAA responsibilities over all non-Intelligence Community IS in the IJOA, including those of USD-C and its subordinate units. (USF-I Directive 25-1, paragraph 2-8 and 3-2, undated (Encl Q5)).

c. (U//~~FOUO~~) Designated Certification Authority. Pursuant to MNF-I Directive 25-1, the DAA for the IJOA may appoint a Designated Certification Authorities to ensure IA and computer network defense (CND) program implementation in the IJOA (MNF-I Directive 25-1, paragraph 6.1.2.9, undated (Encl Q4)). These designated certification authorities approve local issues delegated in writing to them and support the enforcement of security policies and best security practices in their assigned areas (MNF-I Directive 25-1, paragraph 8.2, undated (Encl Q4)). There were no designated certification authorities appointed below the DAA (Email, (b) (6), 9 Feb 11 (Encl O45)).

d. (U//~~FOUO~~) Division G-6/Brigade S-6. Although not specifically designated as a key IA position, the G-6/S-6 exercises overall authority and responsibility for all network operations within his unit's assigned area of operations. The G-6/S-6 works closely with the higher J6/S-6 and subordinate S-6 officers, and the associated signal units to monitor and manage the activities that provide data confidentiality, integrity, availability,

and protection against unauthorized access. (FM 6-02.71, paragraph 3-53, 14 Jul 09 (Encl Q6)). The responsibilities for a G-6/S-6 do not appear in AR 25-1 or AR 25-2.

(1) (U//~~FOUO~~) The 1CD G-6 was LTC [redacted]. (Interview MFR, [redacted], 24 Jan 11 (Encl E34-1)). The 1AD G-6 was LTC [redacted]. (USF-I AR 380-5, Enclosure 13 (Encl R1)).

(2) (U//~~FOUO~~) The 2/10 MTN S-6 was MAJ [redacted]. (USD-C 380-5, Enclosure L (Encl R2)).

e. (U//~~FOUO~~) Information Assurance Manager (IAM). Both CENTCOM and the Army require IAMs to be appointed on orders. The IAM is responsible to execute an organization's IA security program on behalf of the DAA. Organizationally, the IAM .reports directly to the DAA in executing his IA duties. The IAM must be a U.S. citizen, an employee of the U.S. Government, hold a U.S. Government security clearance, and possess access approvals commensurate with the level of information processed by the system under his or her jurisdiction. IAM training and certification requirements vary with the size and scope of the network and systems under their purview. (CCR 25-206, paragraph 7-5.c., undated (Encl Q2); AR 25-2, chapter 3, paragraph 3-2.d., 24 Oct 07 (Encl Q3)). The IAM is responsible for developing and enforcing a formal IA security and training program. (CCR 25-206, paragraph 7-5.c., undated (Encl Q2); AR 25-2, paragraph 3-2.d., 24 Oct 07 (Encl Q3)). For Army units, the IAM is required to conduct security inspections, assessments, tests, and reviews, including subordinate units (CCR 25-206, paragraph 7-5.c., undated (Encl Q2); AR 25-2, paragraph 3-2.d., 24 Oct 07 (Encl Q3)). For Army units, the IAM is required to identify data ownership (including accountability, access, and special handling requirements) for each IS or network within their authority (CCR 25-206, paragraph 7-5.c., undated (Encl Q2); AR 25-2, paragraph 3-2.d., 24 Oct 07 (Encl Q3)). For Army units, the IAM is also required to verify that all the computers under their oversight are properly certified and accredited in accordance with DoD Information Assurance Certification and Accreditation Process (DIACAP) and USF-I configuration management policies and practices. (CCR 25-206, paragraph 7-5.c., undated (Encl Q2); AR 25-2, paragraph 3-2.d., 24 Oct 07 (Encl Q3)).

(1) (U//~~FOUO~~) CENTCOM allows the DAA or the commander to appoint an IAM. Army regulation allows only commanders to appoint IAMs for their designated networks. (CCR 25-206, chapter 7, paragraph 7-5c, undated (Encl Q2); AR 25-2, paragraph 3-2d, 24 Oct 07 (Encl Q3)). The Army's IAM training standards refer back to the standards in DoD 8570.01-M. (DoD 8570.01-M, chapter 4, 19 Dec 05 (Encl Q7)); AR 25-2, chapter 4, paragraph 4-3.a.(3), 24 Oct 07 (Encl Q3)).

(2) (U//~~FOUO~~) CENTCOM had two IAMs. The CENTCOM IAM with specific responsibilities for the CENTCOM headquarters (CCHQ) at MacDill AFB, FL, and the CENTCOM Forward Headquarters (CFH) at Al Udeid Air Base, Qatar, at the time of

PFC Manning's deployment was Ms. (b) (6), (b) (7)(C) . The IAM with AOR-wide responsibilities, less the CCHQ and CFH, was LTC (b) (6), (b) (7)(C) . (Email (b) (6), , 24 Jan 11 (Encl O8)).

(3) (U//~~FOUO~~) The USF-I IAM in mid-2010 was Mr. (b) (6), (b) (7) , who reported to LTC (b) (6), (b) (7)(C) , USF-I J6-Information Assurance Division Chief. Mr (b) (6), had allocated support staff throughout the IJOA to assist division-level IA personnel. This support staff also served as subject matter experts for the division G-6 staffs. (DA Form 2823, (b) (6), 24 Jan 11 (Encl E91-1)).

(4) (U//~~FOUO~~) MAJ (b) (6), (b) served as the IAM for 1CD as MND-B, which was later designated USD-C. (*Interview* MFR, (b) (6), 24 Jan 11 (Encl E21-1)). MAJ (b) (6), (b) (6), was the IAM for USD-C after 1AD took over from 1CD. (Interview MFR, , 23 Jan 11 (Encl E36-1)).

(5) (U//~~FOUO~~) CPT (b) (6), (b) (b)(6) the FA 53, Information Management Systems Officer assigned to 2/10 MTN, arrived at Fort Drum on 1 October 2009, shortly after graduating from the FA 53 Information Systems Management course. He deployed into theater on 14 November 2009, after 2/10 MTN's Transfer of Authority (TOA) with the re-deploying 3d BCT of the 82d Airborne Division. (DA Form 2823, (b) (7)(C) 6 Jan 11 (Encl 13-5)). Upon arrival in theater, CPT (b) (6), (b) assumed duties as the 2/10 MTN IAM. (DA Form 2823, (b) (7)(C) 6 Jan 11 (Encl 13-5)). This was CPT (b) (6), (b) (7) first assignment as a FA 53 officer and his first deployment. He received *some IA training* in the FA 53 course. However, the training was primarily focused on commercial best business practices rather than on the specific duties of an IAM at the tactical level. (Interview MFR, (b) (7)(C) 23 Jan 11 (Encl E13-7); DA Form 2823, (b) (6), (b) 6 Jan 11 (Encl E13-5)).

f. (U//~~FOUO~~) Information Assurance Network Manager (IANM). The Army authorizes the position of IANM in AR 25-2. (AR 25-2, paragraphs 3-2c and e, 24 Oct 07 (Encl Q3)). An IANM must be appointed on orders by the commander, be a U.S. citizen, and hold a U.S. Government security clearance and access approval commensurate with the level of responsibility. The Army's IANM training and credentialing standards follow the Information Assurance Technical (IAT) Level I and II standards established in DoD 8570.01-M. (DoD 8570.01-M, 19 Dec 05 (Encl Q7)). AR 25-2, paragraph 4-3(a)2 enumerates the training requirements for the IANM. (AR 25-2, 24 Oct 07 (Encl Q3)).

g. (U//~~FOUO~~) Information Assurance Security Officer (IASO). The Army requires a commander responsible for IS to appoint an IASO for each IS or group of IS. The same IASO may be appointed for multiple IS. The IASO must achieve and maintain the certification standards in DoD 8570.01-M. (DoD 8570.01-M, 19 Dec 05 (Encl Q7)). The

Army IASO duty position is equivalent to the DoD information assurance officer (IAO) duty position. (AR 25-2, chapter 3, paragraph 3-2.f., 24 Oct 07 (Encl Q3)).

(1) (U//~~FOUO~~) Nothing in CENTCOM Regulation 25-206 mandates appointment of an IAO, although the regulation refers to IAOs in places. USF-I Directive 25-1 mandates appointment of IASOs as required. (CCR 25-206, paragraphs 7-10 and 7-13, undated (Encl Q2)); USF-I Directive 25-1, paragraph 6.4.5, undated (Encl Q5)).

(2) (U//~~FOUO~~) USD-C. Mr. [redacted] was designated as the USD-C IASO, and performed duties at the direction of the IAM. (DA Form 2823, [redacted], 24 Jan 11 (Encl E91-1)). The IASO implements the command's IA program to secure network infrastructure in compliance with IAM guidance, including identification of vulnerabilities, reporting security violations and incidents, network monitoring, and analysis of audit data. (AR 25-2, chapter 3, paragraph 3-2.f., 24 Oct 07 (Encl Q3)).

(3) (U//~~FOUO~~) 2/10 MTN. 2/10 MTN had two IASOs. CW2 [redacted] a MOS 250N Network Management Technician, was appointed an IASO because he held the required CompTIA Security+ credential. (DoD 8570.01-M, Table AP3, 19 Dec 05 (Encl Q7)). However, he did not perform duties as an IASO. (Interview MFR, [redacted] 23 Jan 11 (Encl E25-1)). CW2 [redacted] was on orders as an IASO and performed IASO duties, but had no formal training, other than completion of the on-line SkillPort training. (Interview MFR, [redacted], 23 Jan 11 (Encl E48-1)).

h. (U//~~FOUO~~) System Administrator (SA).

(1) (U//~~FOUO~~) Each SA is appointed on orders by the commander and must be trained, experienced, IA certified, and currently certified on the IS they are required to maintain. The SA should be a U.S. citizen and must hold a U.S. Government security clearance and access approval commensurate with his or her level of responsibility. Training requirements for SAs are found in AR 25-2, paragraph 3-3a. (AR 25-2, 24 Oct 07 (Encl Q3); DoD 8570.01-M, Table AP3, Dec 05 (Encl Q7)).

(2) (U//~~FOUO~~) There were two SAs appointed at 2/10 MTN, both of whom performed administrative tasks including, but not limited to IA scanning and vulnerability assessments and maintaining or suspending user accounts at the direction of the IAM. SGT [redacted], IA NCOIC, served as a SA. SGT [redacted] ran vulnerability scans and reported the results weekly to USD-C. (DA Form 2823, [redacted] 21 Jan 11 (Encl E13-6)). SGT [redacted] was another SA with the same responsibilities as SGT [redacted]. (DA Form 2823, [redacted], 18 Jan 11 (Encl E9-1); DA Form 2823, [redacted] 6 Jan 11 (Encl E13-5)).

i. (U//~~FOUO~~) Information owner/data owner. Each USF-I Major Subordinate Command (which included USD-C) has information owner requirements, similar to the

data owner responsibilities described in AR 25-2. Those requirements include establishing information classification, sensitivity, and access requirements for DoD component-specific information. Information owners are also required to ensure that access to all DoD IS and specific types of information (e.g., intelligence, proprietary) under their purview is granted only on a requirements basis in accordance with DoDD 8500.1. Finally, information owners are required to ensure that DoD component-owned or component-controlled IS are assessed for IA vulnerabilities on a regular basis, and that appropriate IA solutions to eliminate or otherwise mitigate identified vulnerabilities are implemented. The USF-I Major Subordinate Commands were required to report IA issues to USF-I. (MNF-I Directive 25-1, paragraphs 6.3.5., 6.4.10., 6.7.3., and 6.7.4., undated (Encl Q5); USF-I Directive 25-1, paragraphs 6.3.5., 6.4.10., 6.7.3., and 6.7.4., undated (Encl Q4)).

j. (U//~~FOUO~~) All users, regardless of echelon, were required to sign an Acceptable Use Policy and complete the same DoD Information Assurance Training required at their home stations. (USD-C IA Policy Letter 6-1, paragraph 6a, 13 Jan 10 (Encl Q8)). All SAs, network/system managers, and IA personnel were required to undertake training commensurate with DoD 8570.01-M, CCR 25-206, USD-C IA Policy Letter 6-1, and AR 25-2. (DoD 8570.01-M, 19 Dec 05 (Encl Q7); CCR 25-206, undated (Encl Q2), MNF-I Directive 25-1, paragraph 6.7., undated (Encl Q5); USF-I Directive 25-1, paragraph 6.7., undated (Encl Q4), USD-C IA Policy Letter 6-1, paragraph 6a (Encl Q8); and AR 25-2, paragraph 2-8, 24 Oct 07 (Encl Q3)).

3. (U) Information Assurance Training.

a. (U) Institutional training. Each IA workforce position requires specific training courses—some by distance learning and some in resident training courses.

(1) (U//~~FOUO~~) Designated Accrediting Authority (DAA). The Defense Information Systems Agency (DISA) hosts a two-hour DAA training package available via distributed learning. National Defense University also hosts a DAA training course embedded in the CIO certification course taught at Fort McNair. Either of these courses fulfills the minimum training requirement for appointment as a DAA. (DoD 8570.01-M, chapter 5, paragraph. C.5.3., 19 Dec 05 (Encl Q7)).

(2) (U//~~FOUO~~) Information Assurance Manager (IAM). The only Army course of instruction teaching IAM-type duties is the FA 53 course (Information Systems Management), a 30-week course administered by the Signal Center of Excellence at Fort Gordon, Georgia. This course provides instruction geared to attaining the Certified Information Systems Security Professional (CISSP) certificate, and offers students the opportunity to test for the CISSP certificate during the course. The course also teaches some provisions of AR 25-2. (Email (b) (6), (b) , 19 Jan 11 (Encl O9)).

(3) (U//~~FOUO~~) Information Assurance Network Manager (IANM). The Warrant Officer Basic Course and Warrant Officer Advanced Courses for MOS 250N (Network Management Technician) qualify graduates in network management skills and offer some training relevant to IA tasks. However, most instruction focuses on securing Wide Area Networks rather than on IA tasks related to server management. These courses do not adequately address the specific requirements outlined in AR 25-2 paragraph 3-2e (Encl Q3). (Email (b) (6), (b) (7)(C), 19 Jan 11 (Encl O9)).

(4) (U//~~FOUO~~) Information Assurance Security Officer (IASO). The Signal Center of Excellence offers training for the Security+ and CISSP commercial credentials at Fort Gordon (and, through mobile training teams at several remote training sites affiliated with Fort Gordon as well). These courses are both stand-alone courses as well as embedded in most Signal Officer and Warrant Officer training, but are also offered as stand-alone courses. All of the MOS 25B (Information Systems Operator/Analyst) Non-Commissioned Officer Education System (NCOES) courses include Security+ training, as does the MOS 25B AIT. The MOS 25B courses, even in conjunction with a Security+ or a CISSP certificate, do not teach sufficient skills to perform IASO responsibilities in accordance with AR 25-2. The only training pipeline that adequately addresses both the regulatory and knowledge requirements for an IASO is the MOS 255S transition course. However, Warrant Officers do not access directly into MOS 255S. There is no other training that meets all IASO requirements. (NETCOM IA Training BBP, Tables 1 and 4, 6 Aug 10 (Encl Q10)).

(5) (U//~~FOUO~~) System Administrator (SA). The MOS 25B NCOES and AIT courses at Fort Gordon include SA training focus on the Microsoft Server and Client operating systems. Limited security training is included in these courses. Fort Gordon also hosts several stand-alone functional courses focused on the Microsoft model. MOS 25B training for SA duties is adequate for entry-level soldiers completing AIT. (NETCOM IA Training BBP, Tables 1 and 4, 6 Aug 10 (Encl Q10)).

b. (U) Individual (Unit) Training.

(1) (U//~~FOUO~~) There is no Army-mandated IA individual training for units deploying to combat theaters. (FORSCOM G-6 Training Guidance, 17 Aug 09 (Encl Q29)). There is no unit-level individual certification or sustainment training for DAAs, IAM, or IANMs. Those individuals holding commercial certifications required by DoD or Army Regulations are responsible for renewing them as required. (DoD 8570.01-M, paragraph C2.3.7. (Encl Q10); NETCOM IA Training BBP, paragraph 16b, 6 Aug 10 (Encl Q10)).

(2) (U//~~FOUO~~) For IASO and SA positions, the Army CIO/G-6 leases instruction for the Service as a whole through a computer-based instructional website. This site, called SkillPort, offers initial and sustainment training for individuals in IASO and SA

positions, particularly with respect to specific manufacturers' (e.g., Microsoft, Cisco) hardware and software. SkillPort instruction meets the regulatory requirements for individual sustainment training for IASO and SA positions. (NETCOM IA Training BBP, paragraph 16b, 6 Aug 10 (Encl Q10)).

(3) (U//~~FOUO~~) Collective Training. There is no Army-mandated IA collective training for units deploying to combat theaters. (FORSCOM G-6 Training Guidance, paragraphs 2.A through 2.L.13, 17 Aug 09 (Encl Q29)).

4. (U) Information Assurance (IA) Implementation.

a. (U//~~FOUO~~) CENTCOM has overall responsibility for its theater information grid, which includes the certification, accreditation and approval of any changes to the Tier 1 (theater) network of the Global Information Grid (GIG). All network traffic coming out of the CENTCOM AOR goes through CENTCOM to the Tier 0 (global) network controlled by U.S. Strategic Command. CENTCOM mandates that units operating in the USCENTCOM AOR follow their Service's (Army, Navy, Air Force, Marine Corps) IA policies governing network operations and maintenance of command, control, communications, and computers (C4) assets. As a result, Army units deploying into theater were required to implement IA policies and procedures as set forth in AR 25-2. (CCR 25-206, paragraph 7-2, undated (Encl Q2)).

b. (U//~~FOUO~~) USF-I operates and maintains the Tier 1 (theater) network within the IJOA. USF-I also has responsibility for the portion of the Tier 2 (Iraq) network, or internal communications infrastructure for the IJOA, which provides access to the Tier 1 (theater) network and the Defense Information Systems Network (DISN). The USDs and other forces in the IJOA seeking access to the rest of the AOR or outside the AOR (to include the DISN) go through the Tier 2 (Iraq) network for access to the Tier 1 (theater) network. (CCR 25-206, paragraph 2-1d, undated (Encl Q2)).

c. (U//~~FOUO~~) The division-level networks were independent networking environments under the certification and accreditation authority of the USF-I DAA. (DA Form 2823, (b) (6) 24 Jan 11 (Encl E91-1)).

(1) (U//~~FOUO~~) When 1CD deployed into theater in December 2008, MND-B (under its predecessor, 4th Infantry Division) renewed its Authorization to Operate (ATO) under the Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP). The ATO was approved prior to transfer of authority to 1CD and the MND-B domain was integrated into the USF-I enclave, as part of a larger consolidation of networks within the CENTCOM AOR. (Interview MFR, (b) (6) 24 Jan 11(Encl E21-1)).

(2) (U//~~FOUO~~) The 1st Armored Division (1AD) assumed responsibility for the MND-B domain on its TOA with 1CD in January 2010. Brigadier General (BG) Jeffrey G. Smith who commanded 5th Signal Command and served as the DAA for all Army units in Europe, approved the DIACAP package for the 1AD tactical network prior to deployment.[10] Rear Admiral (Lower Half) Simpson, the USF-I DAA, reviewed the signed DIACAP approval and supplemented it with his own DAA memorandum approving the 1AD DIACAP for use at USD-C. (Email (b) (6), , 20 Jan 11, attached to Interview MFR, (b) (6), , 23 Jan 11 (E86-1)). USF-I had responsibility for tactical extensions from the USF-I Tier 2 (Iraq) enclave. (CCR 25-206, paragraph 2-1d., undated (Encl Q2)).

(3) (U//~~FOUO~~) The Host-Based Security System (HBSS), a program that monitors, detects, and counters against known cyber-threats, was fielded to the 1AD/USD-C division headquarters and most of its subordinate brigades in July-August 2010, after PFC Manning's apprehension. 2/10 MTN did not receive HBSS as it was pending redeployment out of theater. (Interview MFR, (b) (6), , 23 Jan 11 (Encl E36-1); (Email (b) (6), , 20 Jan 11, attached to Interview MFR, (b) (6), , 23 Jan 11 (E86-1)).

d. (U//~~FOUO~~) 2/10 MTN deployed to the IJOA in October 2009 and was placed under the operational control of MND-B. They operated their tactical network in theater as an extension to the USF-I Tier 2 network infrastructure. The MND-B information assurance staff exercised oversight of the brigade networks subordinate to MND-B. (Interview MFR, (b) (6), , 24 Jan 11 (Encl E21-1)).

(1) (U//~~FOUO~~) Prior to deployment, 2/10 MTN operated its tactical network during two mission rehearsal exercises at the Joint Readiness Training Center (JRTC) at Fort Polk, Louisiana and for several weeks at Fort Drum. During 2/10 MTN's 2009 JRTC rotations, they were not provided training scenarios specifically relating to IA. According to the COL (b) (6), (b) (7)(C) , the FORSCOM G-6, JRTC focuses on "individual tasks" and "[n]ot much collective IA training tasks." (Email, FORSCOM G-6, 27 Jan 11 (Encl O15)). COL (b) (6), (b) added that the training was "kinda embedded in some of the IOM (install, operate, and maintain) tasks." (Email, FORSCOM G-6, 27 Jan 11 (Encl O15)).

(2) (U//~~FOUO~~) 2/10 MTN deployed to the IJOA in October 2009. The brigade fell under the direct command and control of MND-B with MNF-I and CENTCOM acting

[10] (U) In 2007, DIACAP replaced the DITSCAP process as the established method for the certification and accreditation of IS and network in DoD.

as the next two higher headquarters.[11] 2/10 MTN inherited the network structure from 3/82 ABN, the outgoing unit. (Interview MFR, [redacted], 23 Jan 11 (Encl E34-1)).

(3) (U//~~FOUO~~) 2/10 MTN operated without the certification and accreditation of its network in theater, in violation of CCR 25-206, MNF-I Directive 25-1 and USF-I Directive 25-1. The brigade tactical network was under the authority of the DAA for the IJOA. (DA Form 2823, [redacted] 24 Jan 11 (Encl E91-1)). 2/10 MTN did not prepare the DIACAP package required for certification and accreditation of its network, and did not have an authorization to operate (ATO) or interim authorization to operate (IATO). (Interview MFR, [redacted] 23 Jan 11 (Encl E13-7)). CPT [redacted] the Brigade IAM, was unaware of the policies governing submission of a DIACAP package and had no experience in preparing one. (DA Form 2823, [redacted] 6 Jan 11 (Encl E13-5)).

(4) (U//~~FOUO~~) Brigades in the IJOA commonly connected to the Tier 2 (Iraq) grid and operated their tactical extensions on the network without formal certification and accreditation by the MNF-I/USF-I DAA. (DA Form 2823, [redacted] 24 Jan 11 (E91-1)). According to LTC [redacted], the current USD-I IA/CND chief, brigades were allowed to connect to the grid without having submitted the required DIACAP package due to operational mission necessity. The brigades did not submit proof of assurance, and did not respond to requests to supply such documentation once they were established on the network. (Email, [redacted], 9 Feb 11 (Encl O45)).

(5) (U//~~FOUO~~) 2/10 MTN never received a formal IA certification and accreditation inspection during its tour, contrary to the guidance in MNF-I Directive 25-1, paragraph 6.4.8. and USF-I Directive 25-1, paragraph 6.4.8. (MNF-I Directive 25-1, undated (Encl Q4); USF-I Directive 25-1, undated (Encl Q5)). 1CD, as MND-B, was preparing for relief in place with 1AD when 2/10 MTN deployed to the IJOA. Accordingly, 1CD did not conduct IA inspections of 2/10 MTN. MND-B did conduct a staff assistance visit to ensure that the brigade had the right tools and processes in place, but the visit was short of a formal DIACAP inspection. (Interview MFR, [redacted] 31 Jan 11 (Encl E34-2)). 1AD, as USD-C, planned an inspection of 2/10 MTN during Easter weekend, 2010, but when the flight slated to transport the inspection team was cancelled, the inspection too fell by the wayside and was never rescheduled. USD-C became focused on an upcoming Department of the Army Inspector General (DAIG) IA inspection and did not conduct an inspection of 2/10 MTN prior to the brigade departing the IJOA. (Interview MFR, [redacted] 23 Jan 11 (Encl E36-1); Interview MFR, [redacted], 23 Jan 11 (Encl E86-1)). Neither MNF-I Directive 25-1 nor USF-I Directive 25-1 mandated

[11] (U) 1st Cavalry Division (1CD) was the unit serving as Multi-National Division-Baghdad (MND-B) from January 2009 to January 2010. United States Division-Center (USD-C) was established from the former MND-B and Multi-National Forces-West (MNF-W). In January 2010, 1st Armored Division (1AD) relieved 1CD in place as USD-C and inherited MND-B policies and procedures. References to MND-B are to 1CD, while references to USD-C are to 1AD. USF-I succeeded MNF-I at the end of Operation IRAQI FREEDOM.

a specific frequency of inspections, but both required an IA inspection of subordinate units.

(6) (U//~~FOUO~~) LTC [redacted] noted that MAJ [redacted] and CPT [redacted] were more attentive to IA concerns, especially at the outset of their tour, than the other brigades he had seen in the IJOA. LTC [redacted] assessed 2/10 MTN's IA efforts as "better than average." (Interview MFR, [redacted] 31 Jan 11 (Encl E34-2)).

(7) (U//~~FOUO~~) When CPT [redacted] discovered personal movies and music on 2/10 MTN SIPRNet computers, he raised the issue to the attention of MAJ [redacted] and LTC [redacted] (2/10 MTN XO). Sometimes these unauthorized movies and music carried "a bunch of viruses along with them." Despite CPT [redacted] efforts to enforce network policy, the placement of personal games and movies on the network appears to have persisted. (DA Form 2823, [redacted] 6 Jan 11 (Encl E13-5); DA Form 2823, 21 Jan 11 (Encl E13-6); Interview MFR, [redacted] 23 Jan 11 (Encl E13-7)). LTC [redacted] was fully aware of the efforts to remove unauthorized media from the SIPRNet and he informed COL [redacted] of his plan to do so. (DA Form 2823, [redacted] 20 Jan 11 (Encl E56-1); Interview MFR, [redacted] 10 Jan 11 (Encl E45-1)).

e. (U//~~FOUO~~) Knowledge Management.

(1) (U//~~FOUO~~) MND-B had a knowledge management plan at the division level. Under MND-B, the policy was to keep information channels as open as possible to maximize sharing of information. (Interview MFR, [redacted], 23 Jan 11 (Encl E34-1)).

(2) (U//~~FOUO~~) Under USD-C policy, administrators were required to configure critical network servers for systems security, and analyze and review the logs for abnormal activity. Finally, data owners were required to configure directory and file level access controls to prevent unauthorized access to data. (USD-C Policy Letter, paragraph 7.e., 13 Jan 10 (Encl Q8); AR 25-2, paragraph 4-5, 24 Oct 07 (Encl Q3)).

(3) (U//~~FOUO~~) A search by the AR 15-6 investigative team for a 2/10 MTN knowledge management plan met with negative results. In the absence of guidelines for the enforcement of access controls based on the level of access required to perform official duties, no user permissions existed to restrict access to files or folders within the 2/10 MTN shared directory. (DA Form 2823, [redacted] 6 Jan 11 (Encl E13-5)). Access was restricted, according to CPT [redacted] sometime between 27 April and 20 May 2010. (AIR, [redacted] 2 Jun 10 (Encl E13-1)).

(4) (U//~~FOUO~~) CPT [redacted] attempted to move 2/10 MTN data to a Microsoft SharePoint server, which employed default access controls to limit access to classified information to only those personnel who needed the information to perform their official duties. CPT [redacted] was unable to generate widespread acceptance of SharePoint

and the members of the brigade continued to use a shared directory ("T-Drive") which was limited to members of the brigade network, but did not enforce access controls beyond that point. (DA Form 2823, [redacted] 6 Jan 11 (Encl E13-5)). It was only after PFC Manning was apprehended that 2/10 MTN instituted access controls on folders to limit access to the data they contained. (DA Form 2823, [redacted] 14 Jul 10 (Encl E13-3)).

(5) (U//~~FOUO~~) Until May 2010, user rights for writing to removable media from SIPRNet were enabled by default. PFC Manning, by virtue of his duties as an all-source intelligence analyst, had work requirements to share his intelligence products with interpreters for ultimate use by Iraqi security forces. Accordingly, he had write access to removable media. After PFC Manning was apprehended, 2/10 MTN instituted limitations on access to data and limited removable media write privileges to select computers and select individuals—usually the OIC or NCOIC of a section—an optional workplace security procedure described in DoDI 8500.2. (DA Form 2823, [redacted] 14 Jul 10 (E13-3)).

5. (U//~~FOUO~~) Army-Wide Response to the Compromise of Classified Information on Wikileaks.

a. (U//~~FOUO~~) The Army published four ALARACT (All Army Activities) messages directing actions related to Wikileaks.

(1) (U//~~FOUO~~) ALARACT 245/2010 (Encl Q12), "Sensitive Information in the Public Domain," was released on 14 August 2010. It reemphasized existing policies regarding appropriate response to the compromise of classified and sensitive but unclassified national security information, but did not publish any new guidance.

(2) (U//~~FOUO~~) ALARACT 246/2010 (Encl Q13), "Application of Information Security Procedures," was released on 17 August 2010. It reemphasized the need for compliance with IA policy guidance contained in AR 25-2 but did not publish any new guidance.

(3) (U//~~FOUO~~) ALARACT 256/2010 (Encl Q14), "Directed Actions to Safeguard Against Unauthorized Information Dissemination," was released on 21 August 2010. This was the first message to direct immediate and follow-on actions necessary to protect against the unauthorized downloading of sensitive information. This message directed all Army activities to immediately review and revalidate who had System Administrator rights and user privileges and to grant those individuals the minimum privileges required for their assigned duties and nothing more. It also directed a review of policies governing the ability to write to removable media and to maximize the limits on this capability to the extent operationally feasible. The message also gave guidance

for deployment of HBSS on all Army networks, both Non-Secure Internet Protocol Router Network (NIPRNet) and Secure Internet Protocol Router Network (SIPRNet)).

(4) (U//~~FOUO~~) ALARACT 260/2010 (Encl Q15), "HQDA EXORD 307-10 ISO Wikileaks Actions to Be Taken by the ACOM, ASCC, DRU, and Army Staff," was released on 26 August 2010 and directed all Army Commands, Army Service Component Commands, Direct Reporting Units, and the Army Staff to take specified actions in response to the publication of classified national security information on Wikileaks. The message:

(a) (U//~~FOUO~~) Announced that AR 381-12 has been revised under a new title as "Threat Awareness and Reporting Program (TARP)," with expected re-publication to occur within 30 days. (AR 381-12, Summary of Change, 4 Oct 10 (Encl Q16)).

(b) (U//~~FOUO~~) Advised that the Secretary of the Army had directed Army Commands, Army Service Component Commands, Direct Reporting Units, and the Army Staff to comply with the three prior ALARACTS issued in response to the Wikileaks disclosures and ALARACT 322/3009 (Encl Q17), which provided ten key indicators of a potential insider threat to the Army.

(c) (U//~~FOUO~~) Required reestablishment of random entry/exit inspection programs for secure areas, to include SCIFs.

(d) (U//~~FOUO~~) Mandated review of command Standard Operating Procedures (SOPs) to ensure full compliance with Army security policies.

(e) (U//~~FOUO~~) Reinforced the requirements for self, supervisor and command reporting of security incidents via the Joint Personnel Adjudication System (JPAS).

(f) (U//~~FOUO~~) Required that all personnel be made aware of the insider threats to DoD and the reporting requirements contained in AR 381-12.

(g) (U//~~FOUO~~) Required the addressees to report the status of actions on the above requirements to the Army G-2 within 60 days of the order.

(h) (U//~~FOUO~~) Directed the Department of the Army Inspector General to "consider adding information assurance and security compliance as a separate inspection item for FY 2011."

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

SECTION III: Leading the New Generation and Understanding Its Culture

1. (U//~~FOUO~~) Cultural Gap. Over the course of this investigation, it became apparent that there is currently a cultural gap between the first-line and mid-level leaders and the Soldiers they lead. I define first-line leaders as squad leaders and mid-level leaders through company commanders. The Soldiers they lead are, in major part, of the so-called *Millennial Generation*. This section addresses the general attributes of the *Millennial Generation*, the cultural differences between first-line and mid-level leaders and the led and the leadership challenges that arise because of those differences. This section will offer some preliminary thoughts regarding how Army leaders might begin to bridge this cultural gap. In formulating my thoughts on this subject, as set forth below, I drew from several informative and thought-provoking discussions with Dr. Marc Sageman. Dr. Sageman is an independent researcher on terrorism and holds various academic positions at the University of Pennsylvania, the University of Maryland and with national think tanks. After graduating from Harvard, he obtained an M.D. and a Ph.D. in sociology from New York University and, since 1994, he has been in the private practice of forensic and clinical psychiatry.

2. (U//~~FOUO~~) Attributes of the *Millennial Generation*. PFC Manning is part of the new cohort of Soldiers who enter military service with attributes and beliefs that differ markedly from those espoused by their predecessors. PFC Manning is a member of the *Millennial Generation*, or a *Millennial* for short; demographers use this catch-phrase to describe the segment of the population born between 1980 and 2000.

a. (U//~~FOUO~~) Net Generation. *Millennials* are also called the "Net generation" because they have no memory of a time when the Internet did not exist. Having grown up with the Internet and its related devices and capabilities, *Millennials* are often said to be the most technologically savvy generation in history. The "New Culture" espoused by *Millennials* is transparent, savvy with social media and isolated from the physical world—leading to the development of strong loyalties in the virtual world.

b. (U//~~FOUO~~) Different Values in the Virtual World. *Millennials* develop values and loyalties in the virtual world that often clash with more traditional values and loyalties in the physical world. Clashes occur because some *Millennials* derive a different value set from their participation in the virtual world. Because the world is virtual, there is no perceived benefit to or need for confidentiality or secrecy, nor is one forced to accept the tangible consequences of one's actions. In their virtual world—comprised of online gaming and blogging—*Millennials* believe it acceptable to act in any way one wishes—their actions generate no perceived consequences for which they may be held to account. The appeal and "freedom" of this virtual world is well illustrated in PFC Manning's internet chats with Adrian Lamo. (Wired.com article, "I Can't Believe What I'm Confessing to You," The Wikileaks Chats, 10 Jun 10 (Encl O10)).

c. (U//~~FOUO~~) "Need to Know" vs. "Need to Share." It is the *Millennials'* commitment to transparency that is also troubling in a military context in which the survival of a Soldier and his unit often depend on denying the enemy access to sensitive intelligence information. Prior to 9/11, access to classified information was based on a "need to know." After 9/11, and particularly after the 9/11 Commission issued its findings, a "need to share" culture developed. (9/11 Commission Report, page 434, undated (Encl O16)). In the aftermath of the 9/11 attacks, the U.S. Government began a practice of sharing intelligence, not just within the IC, but with any and all stakeholders across the greater interagency. Naturally, the military was drawn into this pervasive trend toward information sharing. The diversity and volume of classified national security information spilled in the Wikileaks incident is an unplanned, but predictable outcome of this "need to share." The "need to share" classified national security information remains paramount in appropriate cases. That said, procedures must be in place to safeguard information and deny access to those who are not properly cleared and/or do not have an official need to know. Leaders and those with oversight of personnel with access to classified information must scrupulously enforce access standards.

3. (U//~~FOUO~~) Leadership Challenges. The cultural differences between the first-line and mid-level leaders and young Soldiers reflect a cultural gap, of which PFC Manning may be the bellwether. (Interview MFR, Sageman, 27 Jan 11 (Encl E72-1)).

a. (U//~~FOUO~~) Small Unit Cohesion vs. *Millennial* Attributes. Mid-level leaders of *Millennial* Soldiers are comfortable with hierarchy, in marked contrast to the *Millennials* themselves who may not be (USAToday.com, accessed 26 Jan 11 (Encl O11)). Because the overarching success of the military is grounded in small unit cohesion, a young Soldier who is familiar with, and most comfortable in, the virtual world of the Internet – where the self is praised and individuality as well as transparency are glorified – may be unable to adapt to the military's focus on teamwork and operational and information security.

b. (U//~~FOUO~~) Erosion of Leadership Skills. Exacerbating this cultural gap is the leadership challenge that currently exists. The current crop of first-line and mid-level leadership is proficient in combat; however, leadership in a garrison setting and the execution of administrative duties prove challenging. The 2010 Army study on Health Promotion, Risk Reduction, and Suicide Prevention (HP/RR/SP (Encl O12)) found, "[t]he Army's professional development priorities and operational tempo have eroded the technical skills, communicative skills and experiential knowledge needed to lead/manage effectively in the garrison environment." (HP/RR/SP, page 38 (Encl O12)).

c. (U//~~FOUO~~) Recommended Actions. One recommendation proffered by the HP/RR/SP study team to correct this deficiency was to "ensure PME [professional military education], pre-command courses (PCC) and local CDR/1SG courses provide

leaders with the skills to mitigate the challenges of leading Soldiers in garrison." (HP/RR/SP, page 38 (Encl O12)).

d. (U//~~FOUO~~) Train Leaders on the New Culture. The skills taught and developed at the courses mentioned above should include exposure to and practice in the leadership theories and techniques effective in managing and guiding members of the *Millennial Generation,* integrating them in our Army and leveraging the unique skills and perspectives they possess for the good of the organization.

4. (U//~~FOUO~~) Small Unit Cohesion and the Army Values. In my view, connections between Soldiers, the fabric of any well-disciplined, high performing unit, are the best way to illustrate to *Millennials* that secrets and security are both necessary and appropriate in an Army at war; failure to safeguard sensitive information has the undesired consequence of putting them and their buddies in the unit at risk. Although the Army Values have the potential to begin to address this cultural gap between first-line and mid-level leaders and the led, we must undertake an educated and concerted effort to identify and understand the attributes associated with *Millennials* if we hope ever to bridge the gap fully.

5. (U//~~FOUO~~) Loyalty & Commitment. Conversely, the *Millennial Generation* must begin to understand that service as a Soldier entails adherence to standards and values. Loyalty to nation, obedience to the orders of the chain of command and commitment to the welfare of the small unit are nonnegotiable. Maintaining these standards and values requires some information to be carefully safeguarded. Access to and dissemination of information requires discretion and confidentiality. In a world marked by daily technological advances, voluminous data can be disseminated across the globe easily and quickly. (Defense Science Board 2006 Summer Study on Information Management for Net-Centric Operations, Vol. II, April 2007, page 3 (Encl O39)). The scale and impact of a leak may be exponentially greater than previously imagined. Precautions must be taken to effectively assess the trustworthiness of those who are granted access to the Army's most sensitive information. For those with access, leaders must remain vigilant for behavioral indicators or signs that might call into question an individual's trustworthiness and, take appropriate action to address such indicators or behavioral signs while safeguarding information. As with every challenge confronting our Army, good leadership—more so even than technological skill or mastery of the complexities of IA—is the key to success.

6. (U//~~FOUO~~) Conclusion. Along with the focus on the lost art of leadership in garrison, an emphasis must be placed on team building at all levels—all members of a unit—baby boomer, Generation "X" or *Millennial*—must be made to act and feel part of the team. Additionally, the Army must ensure strong leadership, responsibility and accountability throughout the chain of command—leaders themselves must know, exemplify and enforce the standard.

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

SECTION IV: Findings and Recommendations Relating to Information Assurance, Physical Security, Personnel Security and Behavioral Health

Section IVA: Findings and Recommendations Pertaining to Information Assurance.

1. (U//~~FOUO~~) Findings.

a. (U//~~FOUO~~) 2/10 MTN Deficiencies.

(1) (U//~~FOUO~~) Information Assurance (IA) personnel did not hold all of the credentials required by their positions. 2/10 MTN appointed an Information Assurance Security Officer (IASO), an Information Assurance Network Manager (IANM) (which could be filled by an IASO) and two Systems Administrators (SA), in accordance with paragraph 2.E. of U.S. Army Forces Command (FORSCOM) G-6 training guidance for deploying units, dated 17 August 2009, which restates the requirements of AR 25-2 (FORSCOM G-6 Training Guidance, 17 Aug 09 (Encl Q29)). Although two personnel were appointed on orders as IASOs, only one actually performed IASO duties. CW2 (b) (6), possessed the Security+ commercial certification required by DoD 8570.01-M, but he did not perform IASO duties. While CW2 (b) (6), (b) (7) did not meet the commercial certification requirements for an IASO, he was still fully capable of performing his assigned duties as an IASO and did so.

(2) (U//~~FOUO~~) The 2/10 MTN tactical network was not properly certified and accredited. Although 2/10 MTN adhered to the connection approval process, CPT (b) (6), (b) had not been trained in the preparation of DoD Information Assurance Certification and Accreditation Process (DIACAP) packages and did not prepare one. The failure to prepare and submit a DIACAP package violated CCR 25-206, paragraphs 5-14c(10(a) and 7-16, undated (Encl Q2), MNF-I Directive 25-1, paragraph 6.4.3, undated (Encl Q4), and USF-I Directive 25-1, paragraph 6.4.3, undated (Encl Q5). Completion of a DIACAP package would have provided a disciplined method of determining vulnerabilities, establishing access controls and remediating identified deficiencies.

(3) (U//~~FOUO~~) USF-I did not enforce the requirement to submit a DIACAP package as a prerequisite to connection to the network. While MND-B and USD-C had both been authorized to operate their networks as an extension onto the USF-I network, the brigades had no such authorization, for which the USF-I DAA was the approving authority.

(4) (U//~~FOUO~~) There was no knowledge management plan at 2/10 MTN. The lack of such a plan meant there was no guidance for establishing effective access controls or enforcement of the core principle that only properly cleared users with an

official requirement for information were permitted to access the brigade network. The access control policy on the brigade network's shared directory denied access only by exception. The brigade did not fully implement a more restrictive access control model (via Microsoft SharePoint) until after PFC Manning's apprehension. 2/10 MTN did not fully implement a policy to enforce information owner and data owner responsibilities set forth in MNF-I Directive 25-1, USF-I Directive 25-1, and AR 25-2. (MNF-I Directive 25-1, paragraph 6.2.2, undated (Encl Q5); USF-I Directive 25-1, paragraph 6.2.2, undated (Encl Q4); AR 25-2, paragraph 3-3b, 24 Oct 07 (Encl Q3)). DoDD 8500.01E does not address data owner/management responsibilities and those responsibilities are only partially addressed in AR 25-2 and USF-I Directive 25-1. (USF-I Directive 25-1, paragraph 6.2.2, undated (Encl Q4); AR 25-2, paragraph 3-3b, 24 Oct 07 (Encl Q3)). AR 25-1 does not mandate the creation of a knowledge management plan and only tangentially addresses knowledge management at the tactical level. These regulations need to be expanded and improved to include more robust guidance in these areas.

(5) (U//~~FOUO~~) The presence of movies, music and games on 2/10 MTN SIPRNet computers was in direct violation of MNF-I Directive 25-1, paragraph 6.7.11, undated (Encl Q5), USF-I Directive 25-1, paragraph 6.7.11, undated (Encl Q4) and AR 25-2, paragraph 4-20(d)(3), 24 Oct 07 (Encl Q3). That IA personnel were aware of, and tolerated these violations further contributed to already lax standards of IA and network security.

(6) (U//~~FOUO~~) The presence of movies, music and games itself, notwithstanding CPT (b) (6), (b) (7) efforts to remove them and secure the network, while not a direct contributor to the unauthorized disclosure of classified information, evidence a general failure to enforce the policies set forth in MNF-I Directive 25-1, undated (Encl Q5) and USF-I Directive 25-1, undated (Encl Q4). All signs point to an undisciplined operating environment on the 2/10 MTN network.

(7) (U//~~FOUO~~) CPT (b) (6), (b) made a concerted effort to comply with IA principles. He alerted the 2/10 MTN Executive Officer (XO) to the presence of unauthorized media on the network and made appropriate requests asking higher headquarters to conduct vulnerability assessments. On one occasion, the Regional Computer Emergency Response Team (RCERT)-Southwest Asia (from Kuwait) executed such an assessment. However, CPT (b) (6), (b) (7) lack of training prevented him from fully complying with regulations.

(8) (U//~~FOUO~~) Despite being informed by CPT (b) (6), (b) that unauthorized media was on the 2/10 MTN network, LTC (b) (6), the BCT XO, failed to take appropriate steps to terminate or deter this practice. Although LTC (b) (6), disseminated guidance to the staff to remove unauthorized media from systems, he failed to properly follow up, further contributing to an undisciplined attitude towards the 2/10 MTN network.

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

b. (U//~~FOUO~~) Higher Headquarters Deficiencies.

(1) (U//~~FOUO~~) As successive Division G-6s for 2/10 MTN, both LTC (b) (6), and subsequently LTC (b) (6), had overall responsibility for the tactical network. They were responsible for ensuring that all subordinate units, to include 2/10 MTN, certified and accredited their networks prior to operating on the theater network. They were also responsible to ensure that their subordinate IAMs conducted full IA inspections of 2/10 MTN. LTC (b) (6), and LTC (b) (6), failed to exercise proper supervisory responsibility to ensure that the 2/10 MTN network was certified and accredited in accordance with applicable regulations and to ensure that 2/10 MTN was properly inspected.

(2) (U//~~FOUO~~) As the Division IAMs for 2/10 MTN, both MAJ (b) and MAJ (b) (6), were directly responsible for verifying that all subordinate units, to include 2/10 MTN, certified and accredited their networks prior to operating on the theater network. They were also responsible for conducting full IA inspections of 2/10 MTN. They failed to exercise their responsibility to ensure that the 2/10 MTN network was certified and accredited in accordance with applicable regulations and that 2/10 MTN was properly inspected.

(3) (U//~~FOUO~~) Institutional Deficiencies. Army regulations and doctrine do not adequately address knowledge management and IA requirements for tactical units. The responsibilities of a tactical unit (corps, division, brigade, battalion) G-6/S-6, as enumerated in FM 6-02.71, paragraphs 3-53 and 3-54, 14 Jul 09 (Encl Q6) are authoritative but not prescriptive, leading to confusion over the actual responsibilities associated with these positions. The guidance in AR 25-1 and AR 25-2 is prescriptive but is oriented primarily at the Institutional Army.

c. (U//~~FOUO~~) Training Deficiencies.

(1) (U//~~FOUO~~) Institutional training in 2/10 MTN was inadequate. A recurring trend in IA personnel in 2/10 MTN was a lack of formalized training for their positions. Figure 8 illustrates in graphic form the many deficiencies in the scope and breadth of institutional training provided to IA personnel.

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

AR 25-2 AREAS COVERED	FA24	FA53	BOLC	Signal CCC	MOS 25B	WOBC	WOAC
General Policy							
Software Security							
Hardware, Firmware, and Physical Security							
Procedural Security							
Personnel Security							
Information Systems Media							
Network Security (AR 380-5)							
Incident and Intrusion Reporting (AR 380-5)							
Information Assurance Vulnerability Mgt							
Miscellaneous Provisions							
Certification and Accreditation							
Communications Security							
Risk Management							
Logging and Access Control (AR 380-5)							

Not taught
Taught to AR 25-2 guidelines
Taught, but not to AR 25-2 guidelines

Figure 8: Signal Center of Excellence Training Offered in AR 25-2 Subject-Matter Areas (U//~~FOUO~~)

(2) (U//~~FOUO~~) The BCT S-6 IA personnel were not properly trained. The 2/10 MTN S-6 brigade staff inconsistently applied the IA procedures set forth in AR 25-2. Both MAJ [redacted] (BCT S-6) and CPT [redacted] (BCT IAM) were ill-prepared to handle their IA responsibilities. CPT [redacted] deployed to theater immediately following graduation from the FA 53 course. By the time CPT [redacted] arrived at 2/10 MTN, the BCT had already conducted its relief in place/transfer of authority (RIP/TOA) with the 3/82 ABN. The lack of comprehensive IA training was one reason that IA best practices were not well instituted in 2/10 MTN.

(3) (U//~~FOUO~~) 2/10 MTN had no personnel familiar with the IA regulatory requirements outlined in AR 25-2, paragraph 3-2d(13) which mandates certification and accreditation of the tactical network in accordance with the DIACAP. Brigade IA personnel were unaware of the requirement to generate a DIACAP package or unsure how to do so. As a result, the brigade network did not meet the certification and accreditation requirements of the DIACAP program and the brigade network did not implement the IA controls required to properly secure the network.

(4) (U//~~FOUO~~) Prior to deployment, 2/10 MTN IA personnel had little opportunity to train on critical IA tasks. The complete lack of IA-focused training at the Combat Training Centers (CTCs) contributed to a lack of readiness on the part of BCT IA personnel to perform the IA missions required of them in the IJOA.

(5) (U//~~FOUO~~) FA 53 training is inadequate. Interviews and sworn statements rendered by Signal branch and FA 53 field grade officers in the course of this investigation, especially those of CPT (b) (6), (b) (7)(C) and MAJ (b) (6), (b) (7)(C) indicate that the current FA 53 qualification course does not provide the requisite instruction on certification and accreditation of IS sufficient to prepare personnel to perform IAM duties in accordance with AR 25-2. No other military education or training course includes instruction regarding IAM duties. As a result, FA 53 officers are graduating from their qualification course unprepared for the duties they will face when they serve as an IAM in the field.

(6) (U//~~FOUO~~) LTC (b) (6), (b) (7)(C) observation that 2/10 MTN was "better than average" with respect to IA, as compared to his other brigades, indicates a general lack of institutional knowledge on IA across the Army. The absence of collective training, limited individual training, and orientation of policies towards the institutional Army contribute to this lack of knowledge.

(7) (U//~~FOUO~~) DoDD 8500.01E does not address data owner/management responsibilities and they are only partially addressed in AR 25-2 and USF-I Directive 25-1. 2/10 MTN data owners were not trained on their responsibility to secure their data, whether it was stored locally on an information system or centrally on a shared drive. No knowledge management plan existed to provide guidance to data owners for determining which personnel had a requirement for access to specific classified national security information and AR 25-1 does not prescribe guidance for the development of such a plan. As a result, there were few internal controls preventing PFC Manning from gaining access to data for which he had no official requirement.

(8) (U//~~FOUO~~) DoD 8570.01-M, 19 Dec 05 incorporating change 2, 20 Apr 10 (Encl Q19) is too focused on mandating commercial certifications to meet various IA workforce requirements. These certifications have some utility but do not guarantee a more-qualified IA professional.

d. (U//~~FOUO~~) Materiel.

(1) (U//~~FOUO~~) There were no IA security tools at 2/10 MTN that specifically addressed insider threats. The 1AD headquarters deployed the Host-Based Security System (HBSS), a program that monitors, detects, and counters known cyber-threats, but not until after PFC Manning had been apprehended. 1AD did not deploy it to 2/10 MTN because the brigade was slated to return to home station in the near term. HBSS

may have detected and prevented efforts to search the network for other than official purpose, as well as the subsequent download of information from the SIPRNet. (USF-I 380-5, Findings and Recommendations, paragraph 3.b (Encl R1)).

(2) (U//~~FOUO~~) However, even had HBSS been fielded prior to PFC Manning's extraction of data, it would not have prevented Soldiers from running the data extraction tools built into the SIPRNet sites to search for and pull Afghanistan and Iraq significant activity reports (SIGACTs). Nor would HBSS have stopped Soldiers from using any approved web browser program to manually download content from the varied SIPRNet websites accessible at the time of 2/10 MTN's deployment to Iraq. Even if the HBSS feature that restricts a user's ability to write data to re-writeable media had been activated, an intelligence analyst's duties include providing intelligence for translation. Therefore, as an intelligence analyst, PFC Manning likely would have been granted the rights required to write to removable media.

(3) (U//~~FOUO~~) Arcsight, a security event correlation program, is deployed to all theater network operations and security centers (NOSCs) and RCERTs. Arcsight relies on IA sensors that are not emplaced onto tactical networks because of the additional bandwidth they require to transmit data back to the TNOSC. However, none of PFC Manning's activities would have registered in theater-level Arcsight auditing because everything that he did would have been presumed to fall within the scope of his intelligence analyst duties. Arcsight is not currently configured to detect insider threat behaviors. Reconfiguring Arcsight to do so would require the emplacement of IA sensors subject to intelligence oversight.

(4) (U//~~FOUO~~) Data loss prevention tools offer capabilities for monitoring activity on DoD IS and early detection of insider threat behavior. Although the computer industry has not settled on a single definition of data loss prevention, a working definition from Securosis, an information security research and advisory firm, is that of "products that, based on central policies, identify, monitor, and protect data at rest, in motion, and in use, through deep content analysis." (Securosis paper, 21 October 2010 (Encl O35)). These data loss prevention tools can identify and block certain patterns of user behavior that may be consistent with an insider threat.

e. (U//~~FOUO~~) Information Assurance and the SCIF.

(1) (U//~~FOUO~~) IA rules are not changed for SCIFs. The measures for IA in SCIFs for non-IC networks are the same as for non-SCI facilities. Any changes in IA regulations, procedures or policies to collateral networks like SIPRNet will apply to both SCIFs and collateral work areas, thereby obviating any special requirements for SCIFs.

(2) (U//~~FOUO~~) A two-person control system was not used. 2/10 MTN did not enforce a two-person control system until after PFC Manning was apprehended. The

enforcement of a two-person control system serves as a visible deterrent to insider threat activity, would have increased command oversight of PFC Manning's activities and would have enabled enforcement of proper information handling and storage procedures, as described in DoDI 8500.2, Enclosure 4, Attachment 4, 6 Feb 03 (Encl Q20). Two-person control is an optional measure described in Enclosure 4, attachment 4 of DoDI 8500.2 (Encl Q20).

2. (U//~~FOUO~~) Recommendations.

a. (U//~~FOUO~~) Regulatory Issues.

(1) (U//~~FOUO~~) Recommend that the Secretary of the Army propose to the Secretary of Defense that he direct the Assistant Secretary of Defense (Network and Information Integration) (ASD(NII))/DoD Chief Information Officer (CIO) to convene a working group comprised of representatives of all DoD Components to undertake the revision and update of DoDD 8500.01E (Encl Q1) specifically to address data owner and data manager responsibilities. The Secretary should further ensure that AR 25-2 (Encl Q3) is updated to conform with the revised DoDD.

(2) (U//~~FOUO~~) Recommend that the Secretary of the Army propose to the Secretary of Defense that he direct the ASD(NII)/DoD CIO to convene a working group comprised of representatives of all DoD Components to update DoD 8570.01-M (Encl Q19) to eliminate the manual's singular focus on commercial certification of IA personnel and to develop a military certification requirement for IA that merges the best of the commercial certifications with the practicality and functionality of military requirements in theater.

(3) (U//~~FOUO~~) Recommend that the Secretary of the Army direct the Army CIO/G-6 to update AR 25-1 (Encl Q33) specifically to address the development and implementation of knowledge management strategies in tactical units and to enumerate, in detail, the duties and responsibilities of a tactical unit (corps, division, brigade, battalion) G-6/S-6.

(4) (U//~~FOUO~~) Recommend that the Secretary of the Army direct the Army CIO/G-6 to review and update all IA regulations and policies to ensure uniformity in the definition and application of IA terms and in the functions and duties assigned to IA positions. Further recommend that the Secretary of the Army direct the Army CIO/G-6 and the Deputy Chief of Staff, G-2 to collaborate with a view to harmonizing Army 25-series and 380-series regulations, with specific focus on tactical unit IA requirements and IA personnel duties and responsibilities. Lastly, recommend that OSD and JCS update their IA policies to resolve inconsistencies among service, joint force commander and DoD guidance.

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

(5) (U//~~FOUO~~) Recommend that the Secretary of the Army propose to the Secretary of Defense that he direct a review of CENTCOM/USF-I IA policies, particularly as they apply to network certification and accreditation practices.

b. (U//~~FOUO~~) Training.

(1) (U//~~FOUO~~) Recommend that the Secretary of the Army direct the Commander, U.S. Army Training and Doctrine Command to:

(a) (U//~~FOUO~~) Ensure that all Signal Officer, Warrant Officer and NCO training courses include comprehensive and robust training in all subject matter areas addressed by AR 25-2.

(b) (U//~~FOUO~~) Develop a two-week functional course for entry level IAMs, modeled on S-6 training courses, but specifically designed to train FA 53s and Warrant Officers in the field to standard. Incorporate elements of this functional course into other 25-series courses, particularly into the Signal Captains Career Course and battalion and brigade S-6 staff courses.

(c) (U//~~FOUO~~) Develop a one-week functional course for IASOs to complement the entry-level IAM functional course. Incorporate the IASO course in all MOS 25B training and Warrant Office Basic Course 255A training.

(d) (U//~~FOUO~~) Develop and mandate implementation of an IA collective training plan and include in all CTC training exercises IA-related tasks and events designed to prepare IA personnel for their duties and responsibilities in theater tactical settings, to include the prevention and detection of both insider and conventional external threats.

(2) (U//~~FOUO~~) Recommend that the Secretary of the Army direct the Commanding General, U.S. Army Combined Arms Center, in conjunction with the Army CIO/G-6, to oversee the revision and update of the Signal elective offered as part of Intermediate-Level Education (ILE) to provide state of the art network operations training and further require all Signal officers to complete that elective.

(3) (U//~~FOUO~~) Recommend that the Secretary of the Army ensure that all units exercising training and readiness oversight (TRO) require the inclusion of IA-specific events in subordinate units' pre-deployment training.

c. (U//~~FOUO~~) Materiel. Recommend the Secretary of the Army direct the full fielding of CND and data loss prevention tools such as HBSS and Arcsight. Further recommend that the Secretary of the Army take special care to ensure that the employment of these tools is subject to formal, stringent oversight to ensure compliance with applicable law and policy.

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

Section IVB: Findings and Recommendations Pertaining to Personnel Security

1. (U//~~FOUO~~) Findings.

a. (U//~~FOUO~~) The Army G-2's review of PFC Manning's security clearance process determined that PFC Manning's security clearance background investigation and the adjudication of clearance eligibility were conducted in accordance with the national investigative and adjudicative standards. However, not all relevant information was available during PFC Manning's security clearance process, to include his prior behavioral health issues, his behavioral health issues at basic training and his disciplinary issues at AIT. This was due in part to investigative limitations and the failure of leaders to report derogatory information.

b. (U//~~FOUO~~) PFC Manning made three false statements on his SF 86. He lied when denied having debt, denied having ever been fired from a job, and denied ever having sought professional help for behavioral health issues. The investigator was only aware of the first two.

c. (U//~~FOUO~~) While the background investigation was conducted in accordance with the National Investigative Standards (NIS), those standards are such that the investigator was unable to follow-up on the nature of PFC Manning's $1,472 debt (i.e., he skipped out on his lease) because it did not exceed the acceptable debt standard. Further, PFC Manning informed the investigator that his stepmother had made allegations that PFC Manning threatened her. The investigator conducted a search of police records that yielded no information, but did not follow up with the stepmother. Had the stepmother been interviewed, she may have disclosed that PFC Manning had sought help for behavioral health issues, a fact that he failed to disclose on his SF 86 or during the personal interview component of his background investigation.

d. (U//~~FOUO~~) The security clearance adjudication process did not adequately identify and assess "red flags." Further, and more importantly, the adjudicators did not have access to all relevant information. While this AR 15-6 investigation has the benefit of hindsight, there are several issues that could have been better addressed in the clearance adjudication process.

(1) (U//~~FOUO~~) The National Adjudicative Guidelines state that the adjudication process is the careful weighing of a number of variables known as the "whole person concept." (Intelligence Community Policy Guidance 704.2, Annex A, part II, 2 Oct 08 (Encl Q49)). Adjudicators are charged with considering all available information about the person (past, present, favorable, or unfavorable) and must consider the nature, extent, and seriousness of the conduct, as well as the individual's age and/or maturity at the time of the conduct. Adjudicators are required to start with the "presumption of trustworthiness." They are then charged with reviewing the packet and determining

whether there are any indications that the person would not be trustworthy or reliable. Any adverse finding must be tied to one of the 13 national criteria which may be mitigated in accordance with the guidance. This presumption of trustworthiness causes some challenges when the investigation covers only a minimal number of years. In this case, PFC Manning's background investigation covered only a period of 28 months.

(2) (U//~~FOUO~~) While not addressed as such in the security clearance process, that PFC Manning "skipped out" on his lease should have be considered an act of untrustworthiness. The adjudicative guidelines states "failure or inability to live within one's means, satisfy debts, and meet financial obligations may indicate poor self-control, lack of judgment, or unwillingness to abide by rules and regulations, all of which can raise questions about an individual's reliability, trustworthiness and ability to protect classified information." (USD Memorandum, Subject: Implementation of Adjudicative Guidelines for Determining Eligibility for Access to Classified Information, Guideline F, 30 Aug 06, (Q48)). PFC Manning had a debt of approximately $2,500 which he failed to report. One debt was owed to Coopermill Apartments and totaled $1,472. He also had three other accounts in collection, totaling $929. While the monetary amount of a debt or debts should be considered in determining whether financial concerns preclude an individual from being granted a security clearance, the nature and number of debts need to be examined as well. In this case, according to Army G-2 personnel, the debt was minor and not considered in evaluating PFC Manning's suitability for access to classified information. Debt is considered (no matter the scenario) when other indicators are present (e.g., alcohol/substance abuse, gambling etc.). Per the Army G-2, the fact that PFC Manning vacated his apartment without notice to his landlord and simply left the keys is similar to ignoring debt and is not uncommon. (MFR, Army G-2, Enclosure 3 (Encl O4)). Although I agree that the amount of PFC Manning's debt is relatively small, in my opinion, the fact that he "skipped out" on his responsibilities should have been given more weight in assessing his reliability and trustworthiness. Additionally, there should have been an analysis of the number of debts (four in total) and his rationale for failing to disclose these debts on his SF 86. At a minimum, a follow-up interview should have occurred to clarify the facts and circumstances surrounding his financial indebtedness and failure to report it on his SF 86 e-QIP. Currently, the national investigative standards require the debt to exceed $7,500 before an investigator can make additional contact with the subject. (Email [redacted] 1 Feb 11 (O18)). Investigators should have flexibility, after considering all facts and circumstances known to them at the time, to conduct follow on interviews in situations when the debt in question falls below the thresholds set out in the Adjudicative Guidelines.

(3) (U//~~FOUO~~) Adjudicators did not know about PFC Manning's prior behavioral health issues and were not informed about the concerns associated with PFC

Manning's conduct and his behavioral health that came to the forefront during Basic Training and AIT.

e. (U//~~FOUO~~) PFC Manning's prior behavioral health issues were not identified during his MEPS processing. PFC Manning failed to truthfully answer questions regarding whether he had been evaluated or treated for a behavioral health condition.

f. (U//~~FOUO~~) Continuing Evaluation. Notwithstanding the issues this investigation identified with regard to the security clearance investigation and adjudication processes, the critical failure in the area of personnel security resides with PFC Manning's leaders who did not take appropriate actions when faced with allegations of misconduct, behavioral health issues, and statements made to peers and co-workers regarding his loyalty to the United States and the meaning of the American Flag.

(1) (U//~~FOUO~~) There is no institutional training available for commanders or leaders on their responsibility to continuously evaluate a Soldier's eligibility to access classified information. Further, there is no training designed to prepare and assist leaders to identify when misconduct or other behaviors should trigger a derogatory information report to the Army CCF. AR 381-12 (Encl Q22) was revised in October 2010 in order to capture and disseminate indicators of "insider threat" from a counterintelligence perspective. However, individuals who exhibit lack of judgment or control and/or have been deemed to be a threat to themselves or others may also pose a security threat. Commanders and leaders must be able to identify behaviors that call into question an individual's suitability for access to classified information.

(2) (U//~~FOUO~~) One potential way to raise awareness of the linkage between misconduct and security is to include a block on the *Record of Proceedings Under Article 15, UCMJ*, DA Form 2627, to remind the imposing commander of the need to consider whether the circumstances underlying the Article 15 warrant suspension of, or the initiation of action to revoke, the Soldier's security clearance and provide the commander a designated space in which to record his decision. Also, requiring that copies of Article 15s be furnished to the command G-2 or security manager would provide another mechanism to ensure that appropriate assessments are made and required reporting is executed.

(3) (U//~~FOUO~~) Commanders and behavioral health care providers must be educated on the linkage between behavioral health issues and security risks. Behavioral health issues that became evident during basic training must be fully assessed and addressed. A command-referral to Behavioral Health for "tantrum fits of rage" should result in something more than the Soldier being taught breathing exercises. When a Soldier has a security clearance, especially at the TS/SCI level, commanders and behavioral health care providers must be able to work together to identify when behavioral health issues should result in a derogatory report to CCF.

(4) (U//~~FOUO~~) PFC Manning's outbursts and anger management issues were viewed by MSG (b) (6), as mental health issues. However, it should be noted that his outbursts were also violations of the UCMJ. Specifically, it appears that PFC Manning was frequently disrespectful and insubordinate to his supervisors and arguably committed several assaults.

(5) (U//~~FOUO~~) MSG (b) (6), failure to properly and promptly report to the chain of command the full scope of PFC Manning's conduct, behavioral health issues, disavowal of loyalty to the United States, and the "My Problem" email, denied the command the awareness they needed to take appropriate actions to suspend PFC Manning's access to classified information or to submit a DEROG. However, this lack of communication does not excuse the company chain of command's failure to maintain situational awareness of the issues that were impacting their Soldiers and the mission and their failure to fully investigate and take appropriate action regarding the December 2009 incident.

(6) (U//~~FOUO~~) The Division G-2 put in place a good process to review command referred behavioral health information in order to assist commanders in determining appropriate actions regarding Soldiers' access to classified information. However, no similar process existed at the BCT level, specifically within 2/10 MTN. (Interview MFR, (b) (6), , 24 Jan 11 (Encl E39-1)). This is an indicator, in part, of the level of experience that exists at the Division G-2 as compared to the BCT S-2. It is also an indicator of the impact of modularity on the ability of the Division G-2 to provide effective oversight of his functional counterpart at the BCT.

g. (U//~~FOUO~~) Army G-2 Comprehensive Security Resiliency Program. As briefed to the investigative team, the Army G-2 Comprehensive Security Resiliency program addresses several of the personnel security concerns raised by this investigation. Specifically, by improving and standardizing training, implementing a risk rating tool and creating an automated continuing evaluation system, commanders and leaders will be better equipped to fulfill their responsibilities as set out in AR 380-67, 9 Sep 88 (Encl Q23).

2. (U//~~FOUO~~) Recommendations.

a. (U//~~FOUO~~) PFC Manning's security clearance background investigation and adjudication, together with other pertinent excerpts from this AR 15-6 report should be forwarded to the Joint Reform Effort (JRE) to permit the committee to consider and incorporate in its efforts appropriate findings and recommendations from this report. The JRE is a national effort focused on improving security clearance investigation and adjudicative standards. As DoD and DA are required to follow the national investigative and adjudicative standards, any recommendation to modify these standards must be elevated to the national level. The limits on OPM's ability to investigate a clearance

applicant fully (e.g., no jurisdiction to investigate events that occurred prior to an applicant's 16th birthday or to investigate in foreign countries) comprise an area of concern that should be addressed. The Army's demographic includes many young Soldiers – the vast majority of whom present little or no security risk. For those Soldiers who may present a threat, tightening the investigative standards, particularly when the period of time subject to investigation is severely limited could provide a more sound basis on which to adjudicate the individual's trustworthiness and reliability.

b. (U//~~FOUO~~) Recommend that the Army, in conjunction with DoD, continue to seek authorization to review an individual applicant's cyber behavior as a component of the security clearance investigative process to maximize information to be made available for the adjudication process. Currently, cyber behavior is not reviewed because policymakers have not clearly defined "the legal and privacy limits" applicable to the Army's consideration of an individual's cyber behavior in the investigative and adjudicative process." (Email, (b) (6), (b) 1 Feb 11 (O19)).

c. (U//~~FOUO~~) Review procedures at Military Entrance Processing Stations (MEPS) to determine whether behavioral health issues are being properly identified and evaluated in assessing an applicant's suitability for military service. Further, consider whether more robust behavioral health assessments should be conducted for applicants seeking assignment to certain MOSs with access to highly classified national security information.

d. (U//~~FOUO~~) Review procedures to ensure behavioral health or disciplinary issues arising during basic training and/or AIT are forwarded to the chain of command for further assessment or result in the appropriate DEROGs.

e. (U//~~FOUO~~) Establish a training program in order to ensure that commanders and leaders at all levels understand their responsibilities when managing Soldiers with security clearances. This training should include not only information about the derogatory reporting process, but an enumeration of the factors on which leaders should alert when assessing an individual's suitability for access to classified information. These indicators should include those listed in the newly revised AR 381-12 (Encl Q22), as well as behaviors that may indicate a lack of mental stability, lack of judgment or lack of personal control.

f. (U//~~FOUO~~) Ensure standardized processes are in place by which to notify commanders about individuals receiving behavioral health treatment with a view to facilitating commanders' continuous evaluation of personnel security. The 1AD G-2 put in place a process to review behavioral health information for Soldiers holding a security clearance. This enabled the G-2 to assist the commander in making informed decisions regarding Soldiers' access to classified information. Rather than simply relying on the efforts of an experienced, knowledgeable intelligence officer to put such a program in

place, this process should be formalized in regulation. Any formal process must balance personnel security concerns with the imperative to encourage individuals to seek behavioral health assistance when necessary.

g. (U//~~FOUO~~) Recommend that the Army establish conditions and standards to ensure that commanders understand the connection between certain conduct and an individual's eligibility for access to classified information. Consider modifying the DA Form 2627, *Record of Proceedings Under Article 15, UCMJ*, to require commanders to sign and acknowledge that they have considered the Soldier's actions and how they may relate to the Soldier's security clearance or suitability for access to classified information, and that appropriate action has been taken—ranging from no action to filing a report of derogatory information with the CCF with a view toward initiating clearance revocation.

h. (U//~~FOUO~~) Recommend that the Army continue to support efforts such as the Army G-2's Comprehensive Security Resiliency program. Such initiatives will strengthen the personnel security and information security programs by enabling the commander's use of appropriate means of identifying high-risk behaviors, implementing a more robust security, education and training program within their commands, and by providing tools to better assist commanders and leaders in performing their duties related to safeguarding classified information.

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

Section IVC: Findings and Recommendations Pertaining to SCI Physical Security

1. (U//~~FOUO~~) Findings.

a. (U//~~FOUO~~) Regulatory Issues.

(1) (U//~~FOUO~~) DoD and Army regulations are outdated. DoD 5105.21-M-1 (Encl Q24) predates DCID 6/9 (Encl Q25) by 4 years. AR 380-5 (Encl Q11) predates DCID 6/9 by 2 years. Both the DoD and Army regulations fail to implement DCID 6/9 policy regarding entry/exit inspections, even in the face of DCID 6/9 instructions to Cognizant Security Authorities (DIA for DoD) to establish such policy and procedures. Although DCID 6/9 has been rescinded and will shortly be replaced by Office of Director of National Intelligence, Technical Specifications for Construction and Management of SCIFs, the new ODNI policy contains a similar requirement to incorporate "personnel and package inspection procedures" in SCIF SOPs. (ODNI Draft Tech Spec, paragraph D.7, xx Jan 11 (Encl Q60)).

(2) (U//~~FOUO~~) Army regulations fail to address the impact of modularity and the proliferation of SCIFs at the BCT-level and below. The physical security regulations were written prior to Army modularity and do not account for the number and sophistication of intelligence assets and capabilities located in a BCT. Further, the regulatory oversight provisions that set out duties and responsibilities of security personnel are focused on the senior intelligence officials (SIO) for each unit. By regulation, the SIO should be an O-5 or O-6, which would generally preclude a BCT S-2 (usually an O-4) from being an SIO and executing the corresponding responsibilities. This sets up a situation in which a BCT SSR would report to the DIV SSO, who reports to the DIV SIO; the BCT S-2, who is generally the BCT SSR's supervisor, is nowhere to be found in the SCIF physical security chain of responsibility. The regulations also do not account for BCTs deploying separately from their organic division headquarters, and the corresponding challenges that presents to a Division G-2 charged with providing requisite oversight to his functional counterpart in the BCT.

b. (U//~~FOUO~~) Unit Issues.

(1) (U//~~FOUO~~) This investigation did not uncover any evidence that PFC Manning accessed, downloaded or made an unauthorized disclosure of TS/SCI. While we do not believe that SCI was a part of any unauthorized disclosure, the rules and policies regarding SCI are relevant because PFC Manning is alleged to have downloaded other classified information in a SCIF. This prompted an examination of the physical security measures implemented within the SCIF. Further, although PFC Manning could have downloaded classified information from any SIPRNet computer outside the SCIF, the amount of access (measured in terms of time spent on the SIPRNet computer) that PFC Manning had was directly related to his MOS as an

intelligence analyst and his official duties in the SCIF. That said, commanders and leaders must be aware of the potential security risk associated with all SIPRNet computers, not just those located in SCIFs.

(2) (U//~~FOUO~~) The unit failed to enforce appropriate standards by not strictly enforcing the regulatory prohibition on the use of personally-owned rewritable media in the SCIF. 2/10 MTN personnel should not have been permitted to introduce personally owned rewritable media into the SCIF in violation of DIA policy. (DIA SCIF PED Policy, 25 Aug 06 (Encl Q18)). However, the total lack of SCIF entry and exit inspections precluded the SCI security personnel's informed assessment of the content and capability of media introduced into the SCIF. Even if rewriteable media were deemed necessary to accomplish the 2/10 MTN mission, personally-owned rewriteable media should have been barred absolutely. Further, the insertion of rewritable media into a SIPRNet computer should have resulted in the classification and subsequent handling of that media as classified (AR 25-2, paragraph 4-17, 24 Oct 07 (Encl Q3)). Additionally, 2/10 MTN should have a system to account for the use of government-owned rewriteable media and to mitigate the risk associated with their use. (DIA SCIF PED Policy, 25 Aug 06 (Encl Q18)).

(3) (U//~~FOUO~~) Entry/exit inspections may have served as some deterrent. Entry/exit inspections were not required by DoD or Army regulations, however, as stated in AR 380-5, such inspections (although not required) are an effective tool that can be used in command security programs to deter and detect the unauthorized removal of classified information from a SCIF. (AR 380-5, paragraph 6-36, 29 Sep 00 (Encl Q11)). Further, PFC Manning's repeated reference in his blogs to the lack of physical security at the 2/10 MTN SCIF indicates that a robust entry/exit inspection program may have served to deter some of PFC Manning's alleged activities.

(4) (U//~~FOUO~~) SSR training was inadequate. There exists no standard requirement to regulate the scope and extent of training required for SSRs. Regulations simply state that the SIO must ensure the SSO and SSR are trained to conduct their duties. DIA has developed training for SCI security personnel, but attendance at this training is not mandatory. The training received by 1LT (b) (6) was insufficient. One hour to review over 100 slides and to absorb all of the often technical information those slides contained was inadequate to ensure that an SSR has a complete understanding of his or her duties and responsibilities. As the SSR for a SCIF that was geographically separated from its higher headquarters, 1LT (b) (6) received little or no oversight or guidance in carrying out her responsibilities. Because of this geographic disconnect, 1LT (b) (6) needed to be able to understand and implement all of the necessary safeguards and procedures associated with SCIFs. Therefore, she should have received training commensurate with the 64-hour DIA SCI Special Security Personnel Course rather than the hasty one-hour training she received prior to deployment.

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

(5) (U//~~FOUO~~) Inadequate Oversight from Higher Headquarters. Other than the first accreditation inspection in November 2009, there were no other inspections or staff assistance visits to 2/10 MTN. The reliance by USF-I and USD-C on home station SSR training and appointment might make sense from an operational and manpower perspective; however, these deployed headquarters must ensure that the proper standards are being followed. Inspections or staff assistance visits would provide some oversight, and would assist higher headquarters in fulfilling their responsibilities for the oversight of SCI security measures.

2. (U//~~FOUO~~) Recommendations.

a. (U//~~FOUO~~) Recommend that the Secretary of the Army direct a review of AR 380-5 (Encl Q11) for consistency with current ODNI SCIF policies and consider changes to bring AR 380-5 in line with those policies. The Army should establish mandatory entry/exit or "personnel and package" inspections, to include inspections of SCIF personnel, and require routine inspections and staff assistance visits by higher headquarters.

b. (U//~~FOUO~~) Recommend that the Secretary of the Army propose to the Secretary of Defense that he direct a review of DoD 5105.21-M-1 (Encl Q24) to identify any inconsistency with current ODNI SCIF policies.

c. (U//~~FOUO~~) Recommend that the Army prescribe SCI Physical Security guidance and/or revise Army regulations to ensure appropriate policies are in place for tactical units in a modular Army. Specifically, the guidance should clearly establish the roles and responsibilities of a BCT S-2 with regards to SCI physical security.

d. (U//~~FOUO~~) Recommend Army regulations or policies establish the training standard for SCI Security Personnel. The Army should consider mandating attendance at DIA's SCI Security Personnel Training for all SSOs and SSRs (especially those SSRs who will be operating a SCIF that is geographically separated from its higher headquarters).

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

Section IVD: Findings and Recommendations Pertaining to Behavioral Health

1. (U//~~FOUO~~) Findings.

a. (U//~~FOUO~~) Neither a command-referral nor self-referral to Behavioral Health currently triggers a security clearance assessment for the Soldier concerned. This may be acceptable for self-referrals, but not for command referrals. If a Soldier's behavior is such that a command-referral is warranted, a security clearance assessment should be mandatory. In this case, the chain of command failed to take appropriate action.

b. (U//~~FOUO~~) Current behavioral health regulations and practices are insufficient to provide the necessary guidance regarding an individual with a security clearance. The DA Form 3822 does not address access to classified information. The unapproved "MEDCOM Form 4038" used by PFC Manning's behavioral health providers contained a section regarding access to classified information. However, the form allowed the provider to delete the section and did not require the provider to express an opinion about a patient's access to classified information.

c. (U//~~FOUO~~) Behavioral health care providers lack understanding of when and how behavioral health issues could or should impact a commander's decision to suspend an individual's access to classified information. CPT (b) (6), (b) indicated that he would not have recommended suspension of PFC Manning's access to classified information based on his 22 May 2010 evaluation. During that evaluation, CPT (b) (6), (b) stated that PFC Manning's (b) (6), (b) (7)(C) recommended that a (b) (6), (b) (7)(C) Notwithstanding these rather specific and concerning findings, CPT (b) (6) maintained that he would not have recommended suspending PFC Manning's access to classified information. (Behavioral Health Records, 22 May 10 (Encls M1-26 and M1-27); Interview MFR, (b) (6), (b), 25 Jan 11 (Encl E17-3)). CPT (b) (6), another behavioral health care provider, indicated that he would only recommend suspension of an individual's access to classified information if the behavioral health diagnosis was "psychosis." (Interview MFR, (b) (6), (b) 24 Jan 11 (Encl E90-1)).

2. (U//~~FOUO~~) Recommendations.

a. (U//~~FOUO~~) Providers should discontinue the use of the unapproved and unofficial "MEDCOM Form 4038." MEDCOM should consider revising DA Form 3822 to meet the needs of providers when treating Soldiers with behavioral health problems who have access to classified information.

(1) (U//~~FOUO~~) DA Form 3822 should be modified to include a discrete block requiring the behavioral health care provider to provide his or her assessment of whether the Soldier should have or retain access to classified information. Mandating such an assessment in each and every case would highlight the importance of addressing the "insider threat" and the security of classified information.

(2) (U//~~FOUO~~) Providers should assess the potential impact of a Soldier's diagnosis or condition on continued access to classified information in all behavioral health evaluations, whether self-referred or command-directed. Nothing in MEDCOM Reg 40-38 or on DA Form 3822 mandates use of that form for self–referrals. Thus, there is no mechanism requiring a care provider, in the context of a self-referral, to consider questions that the Army and MEDCOM have deemed critical in context of a Command-Directed Behavioral Health Evaluation. (Interview MFR, (b) (6), (b) (7)(C), 25 Jan 11 (Encl E17-3)).

b. (U//~~FOUO~~) A finding of serious risk to self, others or mission should result in command notification in accordance with DTM 09-006, July 2, 2009 (DTM 09-006) (Encl Q39), a command assessment of the Soldier's suitability for access to classified information and an affirmative determination as to whether a derogatory report should be forwarded to CCF.

c. (U//~~FOUO~~) Behavioral Health Regulations Training Deficiency. Our finding is that the Directive Type Memorandum (DTM) 09-006, Subject: Revising Command Notification Requirements to Dispel Stigma in Providing Mental Health Care to Military Personnel is adequate in its identification of the conditions necessary for behavioral health providers to notify commanders when there is a risk to self, others, or the mission. The issue is in training both the behavioral health providers and the commanders. Recommend the Army review the training on and implementation of DTM 09-006 to ensure behavioral health providers and commanders understand the policies regarding commanders' access to mental health information. This information can be critical for commanders in making decisions regarding individuals' access to classified information.

d. (U//~~FOUO~~) Training.

(1) (U//~~FOUO~~) Behavioral Health Care Providers. Army and MEDCOM must develop enhanced training to heighten awareness within the medical community of indicators of an "insider threat." For example, behavioral health care providers should consider the frequency of the visits by a Soldier, whether that Soldier has prior deployments, what the Soldier does on- and off-duty, whether the Soldier has engaged in prior acts of violence or substance abuse, the Soldier's MOS and whether the Soldier has access to classified information.

(2) (U//~~FOUO~~) Commanders and Leaders. Commanders and leaders must be trained on the differences between self-referrals and command-referrals. Specifically, commanders and leaders must be aware of the information to which they are entitled and the information to which they are not entitled in each situation. Further, commanders and leaders must receive training that assists them in identifying when behavioral health issues should impact an individual's access to classified information. One method to place command emphasis on this issue would be to create a graphic training aid (a wallet card) identifying when commanders should consider a command-referral to Behavioral Health and the differences between a command-referral and a self-referral.

e. (U//~~FOUO~~) Review mandatory disclosure standards. The Secretary of the Army should consider directing the Army medical community to review whether standards for mandatory disclosure to the chain of command are: 1) clear and unambiguous; 2) comprehensive; 3) uniform across the Army; and 4) the subject of appropriate training and emphasis. Finally, the Army medical community should consider the merit of developing enhanced procedures for the evaluation of Soldiers with access to classified information.

f. (U//~~FOUO~~) The Secretary of the Army should recommend that the Secretary of Defense review DoDI 6490.1 and DoDI 6490.4 to determine if they should be revised to require a behavioral health care provider to render a written assessment of a patient's "suitability for access to classified information" as part of each and every behavioral health evaluation and to discuss that assessment with the Soldier's commander, without regard to whether the Soldier self-referred or was command-directed to seek behavioral health care.

g. (U//~~FOUO~~) Any change to behavioral health policy should take into consideration the Report of the DoD Task Force on Mental Health. It is critical that the Army continue its efforts to encourage Soldiers to seek early intervention in addressing their behavioral health concerns. However, the Army must strike an appropriate balance between the needs of the individual and the preservation of our national security. When a Soldier engages in behavior that calls into question his or her reliability or trustworthiness, steps must be taken to limit his or her access to classified information. Further, when a behavioral health care provider determines that an individual is a serious risk to self, others or mission, steps must be taken to safeguard both the individual and national security. (DoD Task Force on Mental Health Report, "An Achievable Vision: Report of the Department of Defense Task Force on Mental Health Final Report," June 2007 (Q67)).

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

SECTION V: Individual Accountability

1. (U//~~FOUO~~) In accordance with my appointment memorandum, I thoroughly investigated the potential individual accountability of those personnel with command or supervisory responsibility for PFC Manning, as well as those with responsibility for the systems and processes that did not operate in accordance with applicable standards or regulations. Specifically, I considered individual accountability for: 1) those personnel in PFC Manning's UCMJ and Administrative Chain of Command; 2) those in PFC Manning's technical (i.e., intelligence/S-2) chain of command/supervision; and 3) those personnel with responsibilities and duties, direct or supervisory in nature, to safeguard and secure both classified and sensitive information, as well as to ensure the security of the network (i.e., SIPRNet) used to store and transfer such information.

2. (U//~~FOUO~~) In making my findings and recommendations, I considered the totality of the circumstances as revealed in this investigation and assessed responsibility. I considered the full range of options available to me as a commander and consistent with paragraph 2c of the 16 December 2010 appointment memorandum. I reached my final decisions only after a comprehensive review of all evidence available to my investigation.

3. (U//~~FOUO~~) My investigation considered the responsibility and accountability of 26 personnel ranging from Division Staff to the BCT Commander, COL (b) (6), (b) (7)(C), to the two Team Leaders with direct oversight of PFC Manning, SPC (b) (6), (b) (7)(C) and SPC (b) (6), (b) (7)(C). At figure 9 below is a list of all personnel that were evaluated for personal responsibility and accountability related to the Wikileaks incident (i.e., an Accountability/ Responsibility Matrix) and my determination as to each.

(b) (5)

5. (U//~~FOUO~~) While the investigation uncovered leadership failures, technical failures, or both by some personnel in the addressing PFC Manning's conduct and behavior,

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

(including conduct warranting his referral to Behavioral Health), none of these failures absolve PFC Manning of any alleged criminal activity.[12]

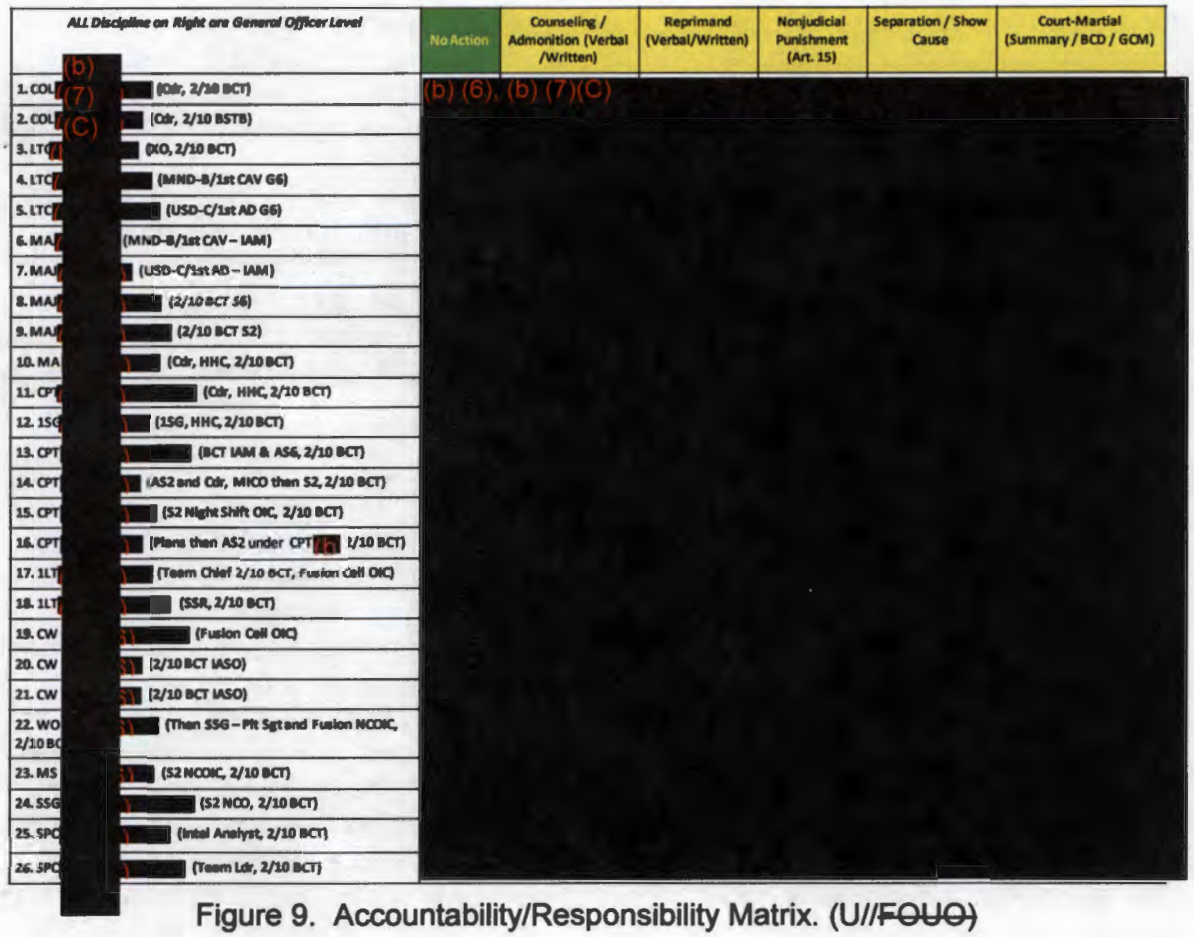

Figure 9. Accountability/Responsibility Matrix. (U//~~FOUO~~)

6. (U//~~FOUO~~) Specific findings and recommendations pertaining to each individual referenced in Figure 9 above are addressed below.

[12] (U//~~FOUO~~) Nothing uncovered during this investigation absolves PFC Manning of personal responsibility for his alleged disclosure of sensitive and classified information. Likewise, nothing uncovered during this investigation regarding PFC Manning's behavioral health issues appears to relieve him of responsibility for his alleged disclosure of sensitive and classified information. Of note – the investigative charter did not include a formal psychiatric assessment of PFC Manning and none was conducted.

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

a. (U//~~FOUO~~) COL [redacted]r (Cdr, 2/10 MTN). As the BCT Commander, COL [redacted] had the ultimate responsibility for everything that happened within his organization. However, after considering all the facts and evidence, I do not find that COL [redacted] was derelict in his duties or otherwise failed to fulfill his responsibilities as a commander. During the course of the investigation, there were four specific areas that I focused on with regard to COL [redacted] 1) COL [redacted] systems and procedures for maintaining situational awareness and oversight regarding his brigade; 2) PFC Manning's deployment, retention in theater and continued access to classified information; 3) the security of the 2/10 MTN SIPRNet; and 4) the decision to retain MAJ [redacted] as Brigade S-2.

(1) (U//~~FOUO~~) I find that COL [redacted] implemented appropriate programs and information gathering measures to understand personnel and problems going on within his organization. PFC Manning's self-referred behavioral health concerns were never elevated to his level of command and COL [redacted] had no reasonable means of obtaining that information absent notification from MSG [redacted] or behavioral health care providers.

(2) (U//~~FOUO~~) PFC Manning. COL [redacted] was the Commander of 2/10 MTN at all times relevant to PFC Manning's service with the BCT. However, prior to the 8 May 2010 assault of SPC [redacted] COL [redacted] had not been informed of PFC Manning's prior misconduct, anomalous behavior, or behavioral health concerns. COL [redacted] was not provided any information by PFC Manning's supervisory chain or subordinate commanders that would have given him reason to question PFC Manning's deployment, retention in theater or continued access to classified information. Further, as PFC Manning had two intermediate commanders, I did not find that COL [redacted] was in a position where he should have known of the incidents related to PFC Manning. When first notified of PFC Manning's assault on SPC [redacted], the new HHC Commander had already taken appropriate action to remove PFC Manning from the SCIF and to initiate UCMJ action. The company commander also initiated a derogatory report through appropriate channels and a command-directed behavioral health evaluation in contemplation of administrative separation for misconduct in accordance with AR 635-200. As COL [redacted] had no knowledge of PFC Manning's behavior, I do not find any failure on his part in regard to this issue.

(3) (U//~~FOUO~~) Security of the 2/10 MTN SIPRNet. LTC [redacted], the 2/10 MTN XO, informed COL [redacted] that there was unauthorized media on the SIPRNet that was impacting network connectivity. LTC [redacted] advised him that the situation was being addressed and that action was being taken to clear the system and obtain better system connectivity. No other issues or concerns regarding the SIPRNet were raised to COL [redacted] level. I find that COL [redacted] properly relied on his XO to address the problems posed by unauthorized media on the SIPRNet.

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

(4) (U//~~FOUO~~) Decision to Retain MAJ [redacted] as Brigade S-2. COL [redacted] was aware that MAJ [redacted] was technically deficient as the S-2 and considered replacing MAJ [redacted] after the July/August 2009 JRTC rotation. However, in consultation with his XO COL [redacted] decided to afford MAJ [redacted] the opportunity to correct his deficiencies, believing that MAJ [redacted] could be successful with his XO's guidance and mentorship. COL [redacted] also designated COL (then LTC) [redacted], the BSTB Commander and a Military Intelligence Officer, as a mentor to MAJ [redacted]. These appropriate measures notwithstanding, COL [redacted] decided, in January 2010, to replace MAJ [redacted] with another officer, CPT [redacted] and moved MAJ [redacted] to a Stability Transition Team (STT). While I find that MAJ [redacted] condoned a dysfunctional leadership style in the S-2 section, I find no inappropriate action or failures by COL [redacted] in his handling of MAJ [redacted], his decision to afford MAJ [redacted] an opportunity to overcome his deficiencies, and COL [redacted] subsequent removal action.

[redacted]

b. (U//~~FOUO~~) COL [redacted] (Cdr, 2/10 BSTB). COL (then LTC) [redacted] BSTB Commander, was the Battalion-level commander for all Soldiers assigned to HHC, 2/10 MTN (PFC Manning's company). After considering all available evidence, I do not find that COL [redacted] was derelict in his duties or otherwise failed to fulfill his responsibilities as a commander.

(1) (U//~~FOUO~~) No Direct Responsibility. COL [redacted] had no direct responsibility for the Brigade S-2, MAJ [redacted] or the S-2 personnel. COL [redacted] was not informed of PFC Manning's prior misconduct, anomalous behavior or behavioral health concerns, and had no reason to know of PFC Manning's behavior. COL [redacted] attempted to provide mentorship and guidance to MAJ [redacted], but in December 2009, finally recommended to COL [redacted] that he remove MAJ [redacted] from the position of S-2.

(2) (U//~~FOUO~~) Contemplated Action: I find COL [redacted] actions in relation to this investigation were reasonable and consistent with that expected of our battalion-level commanders. I specifically find no action or inaction on the part of COL [redacted] warranting administrative or disciplinary action.

c. (U//~~FOUO~~) LTC [redacted] (XO, 2/10 MTN). I find that LTC [redacted] was deficient in his management and supervision of the S-2 section and in his oversight of the security of 2/10 MTN classified network.

(1) (U//~~FOUO~~) Management and Supervision of the S-2 Section. As the XO, LTC [redacted] had the primary responsibility to manage and supervise the varied Brigade

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

Staff Sections, to include the S-2. LTC (b) (6), was deficient in his management and supervision of the S-2 section. Although LTC (b) (6), recognized MAJ (b) (6), (b) technical deficiencies, he failed to recognize that the leadership structure within the entire S-2 Section was dysfunctional. This failure allowed MSG (b) (6), to usurp the authority of both Officers and other NCOs by preventing them from exercising their supervisory responsibilities over the junior enlisted Soldiers in the S-2 Section, to include PFC Manning. He failed to identify the turmoil and trouble pervading the S-2 Section or to root out the "keep it in-house" mindset that existed there. These failures on the part of LTC (b) (6), facilitated MSG (b) (7) ability to hide most of PFC Manning's conduct and anomalous behavior from the Chain of Command.

(2) (U//~~FOUO~~) Oversight of the Security of the Classified Network. The S-6 section informed LTC (b) (6), of the presence of unauthorized media on the classified network. Once informed, LTC (b) (6), took initial steps to address the problem; specifically, he told staff personnel to remove all unauthorized media by a date certain. However, he failed to follow up on his guidance and ensure that no further violations of network security occurred.

(b) (5), (b) (6), (b) (7)(C)

[redacted]

d. (U//~~FOUO~~) LTC (b) (6), (b) (7)(C) (MND-B/1CD G-6).

(1) (U//~~FOUO~~) LTC (b) (6), was the G-6 for MND-B when 2/10 MTN arrived in theater. As the Division G-6 for 2/10 MTN, LTC (b) (6), (b) had overall responsibility for the tactical network. He was responsible for ensuring that all subordinate units, to include 2/10 MTN, were certified and accredited prior to operating on the theater network. LTC (b) (6), failed to exercise proper supervisory responsibility to ensure that the 2/10 MTN network was certified and accredited in accordance with applicable regulations and were properly inspected. At all times relevant to this investigation, the 2/10 MTN network remained uncertified and unaccredited, operating in violation of DoDI 8500.2, CCR 25-206, MNF-I Directive 25-1 and AR 25-2.

(b) (5), (b) (6), (b) (7)(C)

[redacted]

e. (U//~~FOUO~~) LTC (b) (6), (b) (7)(C) (USD-C/1AD G-6).

(1) (U//~~FOUO~~) LTC (b) (6), was the G-6 for USD-C after 1AD relieved MND-B/1CD in place and assumed responsibilities as USD-C in January 2010. LTC (b) (6), had overall responsibility for the tactical network. He was responsible for ensuring that all subordinate units, to include 2/10 MTN, were certified and accredited prior to

operating on the theater network. LTC (b) (6), failed to exercise proper supervisory responsibility to ensure that the 2/10 MTN network was properly certified and accredited for operation and properly inspected. At all times relevant to this investigation, the 2/10 MTN network remained uncertified and unaccredited, operating in violation of DoDI 8500.2, CCR 25-206, USF-I 25-1 and AR 25-2.

(b) (5), (b) (6), (b) (7)(C)

f. (U//~~FOUO~~) MAJ (b) (6), (b) (MND-B/1CD IAM).

(1) (U//~~FOUO~~) As the Higher Headquarters Information Assurance Manager (IAM) for 2/10 MTN, MAJ (b) was directly responsible for verifying that all subordinate units, to include 2/10 MTN, had properly certified and accredited their networks prior to operating on the theater network. MAJ (b) failed to verify that the 2/10 MTN network was properly certified and accredited for operation. Additionally, MAJ (b) (6) failed to conduct required inspections of the network. At all times relevant to this investigation, the 2/10 MTN network remained uncertified and unaccredited, operating in violation of DoDI 8500.2, CCR 25-206, MNF-I Directive 25-1 and AR 25-2.

(b) (5), (b) (6), (b) (7)(C)

g. (U//~~FOUO~~) MAJ (b) (6), (b) (7) (USD-C/1st AD IAM).

(1) (U//~~FOUO~~) MAJ (b) (6), was the IAM for USD-C after 1AD relieved MND-B/1CD in place and assumed responsibilities as USD-C in January 2010. MAJ (b) (6), was directly responsible for verifying that all subordinate units, to include 2/10 MTN, properly certified and accredited their networks prior to operating on the theater network. MAJ (b) (6), failed to verify that the 2/10 MTN network was properly certified and accredited for operation. Additionally, MAJ (b) (6), failed to conduct required inspections of the network. At all times relevant to this investigation, the 2/10 MTN network remained uncertified and unaccredited, operating in violation of DoDI 8500.2, CCR 25-206, USF-I Directive 25-1 and AR 25-2.

(b) (5), (b) (6), (b) (7)(C)

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

h. (U//~~FOUO~~) MAJ [redacted] (S-6, 2/10 MTN).

(1) (U//~~FOUO~~) As the 2/10 MTN S-6, MAJ [redacted] had overall responsibility for the 2/10 MTN network. He was responsible for ensuring that the 2/10 MTN network was properly certified and accredited before operating on the theater network. MAJ [redacted] also had supervisory oversight, with his Assistant S-6, CPT [redacted] over the entire 2/10 MTN network and its operations. MAJ [redacted] failed to exercise proper supervisory oversight and responsibility to ensure timely certification and accreditation of the 2/10 MTN network. At all times relevant to this investigation, the 2/10 MTN network remained uncertified and unaccredited, operating in violation of DoDI 8500.02, CCR 25-206, MNF-I Directive 25-1, USF-I Directive 25-1, and AR 25-2.

[redacted]

i. (U//~~FOUO~~) MAJ [redacted] (S-2, 2/10 MTN).

(1) (U//~~FOUO~~) MAJ [redacted] failed to properly supervise and manage the personnel in the S-2 Section. He abdicated his responsibility to supervise all S-2 personnel, Officer and enlisted, instead deferring to MSG [redacted] his NCOIC, to address all enlisted issues at his level. He allowed, and actively underwrote, MSG [redacted] efforts to strip supervisors, Officers and NCOs alike, of their responsibility over subordinate enlisted personnel. In so doing, he created a dysfunctional and unclear leadership scheme. He also facilitated MSG [redacted] ability to withhold information and decisions to himself, keeping the HHC Company Commander and First Sergeant uninformed regarding misconduct and anomalous behavior by S-2 Section personnel. He also fostered an environment where critical information was hidden from the Chain of Command and kept within the S-2 Section. The dysfunctional environment MAJ [redacted] fostered and encouraged allowed MSG [redacted] to make command-level decisions without command awareness or input, such as: whether to deploy PFC Manning; whether to direct a behavioral health evaluation or to allow the PFC Manning to self-refer; whether disciplinary action would be a consequence of PFC Manning's misconduct; and whether action would be taken to suspend PFC Manning's access to classified information.

[redacted]

j. (U//~~FOUO~~) MAJ [redacted] (Cdr, HHC, 2/10 MTN).

(1) (U//~~FOUO~~) MAJ [redacted] was the HHC Commander from 28 April 2009 to 17 April 2010. He had overall responsibility for the care and discipline of all Soldiers under

his charge (to include PFC Manning), and was required to maintain awareness of all situations that might adversely affect the mission or the well-being of his personnel. Despite having a critical leadership role, MAJ [redacted] was woefully ignorant of PFC Manning's actions and the impact they were having on the S-2 Section. Likewise, MAJ [redacted] was woefully ignorant of the impact MSG [redacted] actions were having on the S-2 Section and its personnel. Despite being uncertain as to whether his First Sergeant was aware of what was happening in the S-2, MAJ [redacted] willingly abdicated his own responsibility for command oversight. MAJ [redacted] only command involvement regarding PFC Manning appears to be his decision to direct PFC Manning to submit to a behavioral health evaluation after his 20 December 2009 outburst in the SCIF. MAJ [redacted] failure as a leader extended beyond his ignorance of PFC Manning's situation. He willingly and knowingly abdicated his responsibility over enlisted personnel issues to the various section NCOICs, in essence delegating his non-delegable command authority. Making matters worse, MAJ [redacted] failed to check on, manage and supervise those personnel to whom he delegated his authority, MSG [redacted] in the S-2 Section among them. MAJ [redacted] was ignorant of the real command structure within the S-2 Section and the impact that MSG [redacted] was having on operations and the morale and welfare of his Soldiers.

[redacted]

k. (U//~~FOUO~~) CPT [redacted] (Cdr, HHC, 2/10 MTN).

(1) (U//~~FOUO~~) CPT [redacted] assumed command of HHC in April 2010 from MAJ [redacted] Immediately upon becoming aware of PFC Manning's misconduct (i.e., the 8 May 2010 assault upon SPC [redacted]), CPT [redacted] took decisive and immediate action to remove PFC Manning from the SCIF, to initiate a command-directed behavioral health evaluation in contemplation of administrative separation for misconduct in accordance with AR 635-200, and to administer a Company Grade Article 15 for PFC Manning's misconduct. CPT [redacted] also completed a DA Form 5248-R, *Report of Unfavorable Information for Security Determination,* to suspend PFC Manning's access to classified information. CPT [redacted] took these actions within 48-hours of the assault on SPC [redacted] and before any allegation arose as to the potential compromise of classified information by PFC Manning.

[redacted]

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

l. (U//~~FOUO~~) 1SG [redacted] (1SG, HHC, 2/10 MTN).

(1) (U//~~FOUO~~) 1SG [redacted] like MAJ [redacted] managed from afar, lacking the situational awareness necessary to accomplish the mission and take care of Soldiers. As the HHC 1SG from the time that PFC Manning arrived at the unit until March 2010, he had primary responsibility for the enlisted Soldiers under his charge and was required to maintain situational awareness of all situations that might adversely affect the mission or the well being of his personnel. Despite having a critical leadership role, 1SG [redacted] was ignorant, either willfully or through neglect, of PFC Manning's actions and the impact they were having on the S-2 Section. Likewise, 1SG [redacted] was ignorant of the impact MSG [redacted] actions were having on the S-2 Section and its personnel. 1SG [redacted] willingly abdicated his responsibility to provide command oversight over the S-2 Section. 1SG [redacted] only involvement with PFC Manning appears to have been a counseling session following his 20 December 2009 outburst in the SCIF. 1SG [redacted] failed to recommend any further inquiry or investigation into the incident and failed to consider whether PFC Manning should continue to have access to classified information. 1SG [redacted] failure as a leader extended beyond the handling of PFC Manning's anomalous behavior. He willingly and knowingly abdicated his responsibility over enlisted personnel issues to the various section NCOICs. 1SG [redacted] failed to check on, manage and supervise those NCOs subordinate to him, including MSG [redacted] in the S-2 Section. 1SG [redacted] was unaware of the fact that MSG [redacted] had usurped the role of Officers and other NCOs alike in making PFC Manning his sole responsibility. 1SG [redacted] lack of command presence in the S-2 Section created an unacceptable gap in leadership stemming from his unreasonable reliance on others to take care of enlisted matters. According to 1LT [redacted], it appeared as if the 1SG didn't care about the S-2 Section because the 1SG and S-2 Section were not co-located. While I believe 1SG [redacted] and MAJ [redacted] leadership failures mirror each other, ultimate responsibility for running a Company resides with the Commander. If MAJ [redacted] performed his duties as expected, perhaps 1SG [redacted] would have done so as well.

(b) (5), (b) (6), (b) (7)(C) [redacted]

m. (U//~~FOUO~~) CPT [redacted] (IAM and AS-6, 2/10 MTN).

(1) (U//~~FOUO~~) As the 2/10 MTN Assistant S-6 and Information Assurance Manager, CPT [redacted] had responsibility for the 2/10 MTN network and its security. He was responsible for ensuring that 2/10 MTN's network was properly certified and accredited before operating on the theater network. CPT [redacted] had direct oversight over the entire 2/10 MTN network and its operations. CPT [redacted] failed to take the requisite measures to timely certify and accredit the 2/10 MTN network and failed to adequately secure the network as it was his duty to do. At all times relevant to this

investigation, the 2/10 MTN network remained uncertified and unaccredited, operating in violation of DoDI 8500.2, CCR 25-206, MNF-I Directive 25-1, USF-I Directive 25-1 and AR 25-2.

[redacted]

n. (U//~~FOUO~~) CPT [redacted] (AS-2 and Cdr, MICO, then S-2, 2/10 MTN).

(1) (U//~~FOUO~~) Upon deployment with 2/10 MTN, CPT [redacted] was serving as both the Assistant S-2 (AS-2) and the Military Intelligence Company Commander. He had served in these positions from 6 February 2008 through January 2010. As the AS-2 he had or should have had situational awareness of all personnel-related issues within the S-2 Section. He also had the ability to influence and supervise S-2 operations. On or about 1 January 2010, CPT [redacted] assumed duties as the Brigade S-2. During his time as AS-2 and S-2, CPT [redacted] allowed MSG [redacted] to personally handle enlisted personnel issues, to include those related to PFC Manning, to the exclusion of the Chain of Command (i.e., Company Commander and First Sergeant). CPT [redacted] allowed MSG [redacted] to effectively "cut out" PFC Manning's first and mid-level supervisors from participating in decisions regarding his care and discipline. Additionally, while AS-2 and S-2, CPT [redacted] allowed unauthorized media to be placed on the classified network and failed to take decisive corrective action in a timely manner. Finally, CPT [redacted] failed to ensure that classified materials were not removed from the SCIF for non-official purposes.

(2) (U//~~FOUO~~) While serving in multiple positions and transitioning between several key positions, CPT [redacted] faced significant challenges as noted above. Once afforded the opportunity to focus on his S-2 duties, CPT [redacted] took responsibility for the S-2 section and immediately identified the lack of leadership for Soldiers on the night shift. He implemented a plan to have MSG [redacted] perform swing shift duties to address that issue. In addition, he moved PFC Manning to the day shift, where PFC Manning's conduct could be managed by supervisors. CPT [redacted] took action to reorganize the S-2 section in a manner that allowed the Brigade to conduct its overall mission more efficiently.

[redacted]

o. (U//~~FOUO~~) CPT [redacted] (S-2 Night Shift OIC, 2/10 MTN).

(1) (U//~~FOUO~~) CPT [redacted] was a branch-detailed Military Intelligence officer who deployed immediately to Iraq after arriving at Fort Drum from his transition course in October 2009. Shortly after his arrival at 2/10 MTN, he was made the officer-in-charge

(OIC) of S-2 night operations, a position he held for less than five weeks before being moved to a battalion intelligence section. During that time, PFC Manning exhibited no conduct warranting action on CPT [redacted] part.

[redacted]

p. (U//~~FOUO~~) CPT [redacted] (S-2 Plans and then AS-2, 2/10 MTN).

(1) (U//~~FOUO~~) CPT [redacted] served as an S-2 Plans intelligence officer and then as Assistant S-2 under CPT [redacted] after he assumed duties as S-2 in January 2010. Although she would task PFC Manning and those in the fusion cell, CPT [redacted] had no supervisory responsibility over PFC Manning until she assumed the role of AS-2. From the time of CPT [redacted] assumption of duties as AS-2 until PFC Manning's assault on SPC [redacted] PFC Manning exhibited no conduct warranting any action on her part. Although PFC Manning sent two emails that should have raised red flags during CPT [redacted] time as AS-2, CPT [redacted] neither knew, nor had reason to know, of the emails or their content.

[redacted]

q. (U//~~FOUO~~) 1LT [redacted] (S-2 Team Chief, 2/10 MTN).

(1) (U//~~FOUO~~) 1LT [redacted] deployed to Iraq in February of 2010. She was originally made the Sunni Team Chief and later the OIC for the fusion cell. From February through 8 May of 2010, 1LT [redacted] performed her duties and cared for the Soldiers under her charge. Although she had heard stories about PFC Manning, there were no incidents involving PFC Manning during this period that required action on her part. On 8 May 2010, however, the day after PFC Manning assaulted SPC [redacted] 1LT [redacted] noticed PFC Manning walking with MSG [redacted] while still in the possession of his weapon. 1LT [redacted] concerned for the safety of her Soldiers and believing that appropriate action had not been taken to address the assault on SPC [redacted] took the initiative to contact the Brigade Judge Advocate and the Commander to advise them of the assault and her current concerns about PFC Manning. As a result of her direct action, CPT [redacted] was able to take timely and appropriate action to remove PFC Manning from the SCIF, command-direct PFC Manning for behavioral health evaluation,

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

administer nonjudicial punishment and complete a DA Form 5248-R, *Report of Unfavorable Information for Security Determination*, to suspend PFC Manning's access.

[redacted]

r. (U//~~FOUO~~) 1LT [redacted] (SSR, 2/10 MTN).

(1) (U//~~FOUO~~) 1LT [redacted] was on orders as the 2/10 MTN SCIF Special Security Representative (SSR). Upon deployment, she allowed MSG [redacted] to handle the SSR's physical security duties while she handled security clearance issues (e.g., security clearance reviews of personnel accessing the SCIF). This investigation found no evidence that MSG [redacted] was either appointed as an SSR or that he ever attended SSR training prior to or during the deployment. As the SSR, 1LT [redacted] had overall direct responsibility for both the physical security of the SCIF and personnel security issues affecting the SCIF. Her duties included the obligation to take immediate and decisive action to correct security deficiencies such as the introduction of personal media into the SCIF and their use on SIPRNet computers. As the SSR, 1LT [redacted] should have identified SCIF security issues, concerns and vulnerabilities and taken measures to remedy or address them. She failed in her SSR duties.

[redacted]

s. (U//~~FOUO~~) CW2 [redacted] (Fusion Cell OIC).

(1) (U//~~FOUO~~) CW2 [redacted] was the fusion cell team leader with responsibility and oversight over WO1 (then SSG) [redacted] as well as PFC Manning. Notwithstanding his positional authority and authority commensurate with his rank, CW2 [redacted] failed to properly exercise that authority. Throughout the period that PFC Manning was subject to CW2 [redacted] leadership, CW2 [redacted] was aware of numerous issues related to PFC Manning's conduct and behavior. Yet, CW2 [redacted] took no action to address any of these issues. CW2 [redacted] rationale for not taking appropriate action was that MSG [redacted] was handling all Soldier issues. When MSG [redacted] failed to take appropriate action regarding PFC Manning's conduct and behavior, CW2 [redacted] still did nothing. CW2 [redacted] was a supervisor in name only, abdicating his responsibilities over PFC Manning to MSG [redacted] When MSG [redacted] failed to take timely and appropriate action regarding PFC Manning, CW2 [redacted] neither notified the chain of command of the numerous issues he observed nor took action himself to address the issues.

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

(b) (5), (b) (6), (b) (7)(C)

t. (U//~~FOUO~~) CW2 (b) (7)(C), (b) (IASO, 2/10 MTN).

(1) (U//~~FOUO~~) CW2 (b) (6), was formally assigned as one of 2/10 MTNs Information Assurance Security Officers (IASOs). He was detailed to this position because he had completed a commercial certification course, "Security+." Notwithstanding his designation as IASO, he did not perform these duties nor was he expected to perform these duties during the deployment. Rather, he performed the duties of Information Assurance Network Manager (IANM). The Investigation revealed that CW2 (b) (6), conducted his IANM duties in accordance with applicable policies and regulations.

(b) (5), (b) (6), (b) (7)(C)

u. (U//~~FOUO~~) CW2 (b) (6), (b) (7) (IASO, 2/10 MTN).

(1) (U//~~FOUO~~) CW2 (b) (6), was formally assigned as one of 2/10 MTNs Information Assurance Security Officers (IASOs). The Investigation revealed that CW2 (b) (6), conducted his IASO duties in accordance with applicable policies and regulations.

(b) (5), (b) (6), (b) (7)(C)

v. (U//~~FOUO~~) WO1 (b) (6), (b) (7)(C) (Formerly SSG/Plt Sgt and S-2 Fusion Cell NCOIC).

(1) (U//~~FOUO~~) WO1 (then SSG) (b) (6), was PFC Manning's Platoon Sergeant pre-deployment and retained that position through 11 February 2010, while 2/10 MTN was deployed. His position vested him with supervisory authority over PFC Manning; however, he failed to properly exercise that authority. Notwithstanding his positional authority as Platoon Sergeant and his knowledge of PFC Manning's numerous issues while under his leadership, WO1 (b) (6), took no action to address PFC Manning's conduct or behavior. His rationale for not taking appropriate action was that MSG (b) (6), had told him that he (SSG (b) (6), (b) was PFC Manning's technical supervisor

only, responsible only for PFC Manning's work product, and that all Soldier issues affecting PFC Manning would be handled by MSG [redacted] himself. When MSG [redacted] failed to take appropriate action regarding PFC Manning's conduct and behavior, however, WO1 [redacted] did nothing, content with his role as technical supervisor only. WO1 [redacted] abdicated his responsibilities over PFC Manning to MSG [redacted] and then failed either to notify the chain of command of the numerous issues he observed or to take appropriate action to address those issues, to include PFC Manning's alleged violence toward other Soldiers and repeated FTRs.

[redacted]

w. (U//~~FOUO~~) MSG [redacted] (S-2 NCOIC, 2/10 MTN).

(1) (U//~~FOUO~~) MSG [redacted] was the NCOIC of the 2/10 MTN S-2 Section. He was responsible for the day to day administrative supervision and leadership of enlisted personnel within the staff section.

(2) (U//~~FOUO~~) MSG [redacted] Supervisory Environment. In a traditional unit, leaders are expected to counsel Soldiers, address deficiencies, recommend both awards and, when appropriate, discipline, and perhaps most importantly, keep the UCMJ Chain of Command informed of those issues affecting the well being and behavioral health of Soldiers within the formation. MSG [redacted] whose approach to leadership appeared to be hands on, close, and personal, became too close to PFC Manning, losing the necessary objectivity to effectively lead Soldiers both in Garrison and during a deployment. This loss of objectivity resulted in MSG [redacted] directing the other leaders with responsibility for PFC Manning (such as PFC Manning's Platoon Sergeant and Section OIC) to leave all Soldier issues regarding PFC Manning to MSG [redacted] himself. MSG [redacted] effectively stripped key leaders of any responsibility over PFC Manning other than technical responsibility for intelligence-related products. MSG [redacted] loss of objectivity, coupled with his decision to truncate and modify the doctrinal Chain of Command and supervision over PFC Manning, resulted in the failure of critical information to flow to the UCMJ Chain of Command.

(3) (U//~~FOUO~~) Failure to Keep Command Informed. MSG [redacted] elected to keep information related to PFC Manning to himself and to handle all of PFC Manning's issues at his level. When the question of whether to deploy PFC Manning arose, MSG [redacted] in consultation with the S-2, decided to deploy the Soldier. The Chain of Command was not informed. When PFC Manning was struggling with behavioral health issues, MSG [redacted] handled the situations without advising the command, recommending that PFC Manning self-refer to Behavioral Health, thus limiting the information available to the command. When PFC Manning had emotional outbursts resulting in violence directed at other Soldiers or was disrespectful, MSG [redacted]

handled the situation by merely talking to PFC Manning and not advising the chain of command. When PFC Manning made a statement potentially indicating a lack of loyalty to the United States, further stating that the United States flag meant nothing to him, MSG (b) (6), kept the information from the Chain of Command and failed to take any action to affect PFC Manning's access to classified information. Even after PFC Manning sent an email to MSG (b) (6), with a photo of himself wearing a blond wig and make-up, MSG (b) (6), did nothing to notify the Chain of Command.

(4) (U//~~FOUO~~) Failure to take appropriate actions after PFC Manning assaulted SPC (b) (6), (b) Twenty-four hours after PFC Manning had assaulted another Soldier in the SCIF, MSG (b) (6), was observed "walking" with him and allowing PFC Manning to retain possession of his weapon and ammunition. MSG (b) (6), again failed to notify the Chain of Command. In short, MSG (b) (6), had countless opportunities to advise the Chain of Command about PFC Manning's conduct, yet repeatedly chose to do nothing, actively taking steps to ensure that he, and only he, handled issues related to PFC Manning. MSG (b) (6), guidance to all others in PFC Manning's supervisory chain was clear–only MSG (b) (6), was to deal with PFC Manning.

(5) (U//~~FOUO~~) Dereliction of Duty. MSG (b) (6), was derelict in his duties as S-2 NCOIC. He kept vital information from the Chain of Command, assuming, in essence, the roles of Section NCOIC, First Sergeant, and Company Commander. He made himself the keeper of all information related to PFC Manning and took on the role of making all critical command decisions regarding PFC Manning, notwithstanding his lack of command authority. MSG (b) (6), with limited consultation with the S-2, decided to deploy PFC Manning. MSG (b) (6), decided to allow PFC Manning to self-refer to Behavioral Health. MSG (b) (6), decided whether the command should be informed about PFC Manning's conduct and behavior. MSG (b) (6), decided not to inform the command about an email from PFC Manning that should have caused a reasonable intelligence section NCOIC to believe that PFC Manning had significant behavioral health problems. Finally, through tactics designed to fence-off PFC Manning from involvement with other leaders and his own protectiveness of PFC Manning, MSG (b) (6), allowed PFC Manning to retain access to classified information. As a result, key leaders did not have a complete picture of PFC Manning. Had those leaders been made aware of PFC Manning's conduct and behavior, that knowledge should have led them to suspend his access to classified information or to initiate the revocation of his security clearance.

(b) (5), (b) (6), (b) (7)(C)

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

(b) (5), (b) (6), (b) (7)(C)

x. (U//~~FOUO~~) SSG [redacted] (S-2 NCO, 2/10 MTN).

(1) (U//~~FOUO~~) SSG [redacted] exercised administrative supervisory responsibilities over PFC Manning prior to 2/10 MTN's deployment in October of 2009. From October of 2009 until March of 2010, SGT [redacted] did not work in the SCIF and did not exercise any administrative or supervisory control of PFC Manning. In March of 2010, SGT [redacted] was made the platoon sergeant and was responsible for counseling PFC Manning after the 8 May 2010 assault on SPC [redacted]

(b) (5), (b) (6), (b) (7)(C)

y. (U//~~FOUO~~) SPC [redacted] (Team Ldr, S-2, 2/10 MTN).

(1) (U//~~FOUO~~) SPC [redacted] performed duties as PFC Manning's immediate supervisor in November and December 2009. During his time as PFC Manning's supervisor, he and PFC Manning were of equal rank. PFC Manning was not reduced from SPC to PFC until his Company Grade Article 15 on 24 May 2010 (relative to his assault on SPC [redacted] on 8 May 2010). At the time he exercised supervisory duties over PFC Manning, SPC [redacted] had not yet attended any Army leadership schools or training. His exact role regarding PFC Manning was unclear as evidenced by the fact that he had to ask MSG [redacted] and SSG [redacted] for permission to counsel PFC Manning. Additionally, the exact supervisory chain in the SCIF was unclear. SPC [redacted] role as PFC Manning's supervisor ended after the table-flipping outburst in December of 2009.

(b) (5), (b) (6), (b) (7)(C)

z. (U//~~FOUO~~) SPC [redacted] (Team Ldr, S-2, 2/10 MTN).

(1) (U//~~FOUO~~) SPC [redacted] performed duties as PFC Manning's immediate supervisor, both pre-deployment and for two months at the beginning of the deployment (i.e., October-November 2009). During her time as PFC Manning's supervisor, she and PFC Manning were of equal rank. PFC Manning was not reduced from SPC to PFC until his Company Grade Article 15 on 24 May 2010.

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

(b) (5), (b) (6), (b) (7)(C) [redacted]

ROBERT L. CASLEN, JR.
Lieutenant General, USA
Investigating Officer

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

SECTION VI: Appendices

Appendix 1: Personnel Listing

Individual	Organization	Location
COL (b) (6), (b) (7)	Headquarters, 2d Brigade Combat Team, 10th Mountain Division	Fort Drum, NY
COL (b) (6), (b) (7)(C)	Headquarters, US Army Medical Command	Fort Sam Houston, TX
COL (b) (6), (b) (7)	Headquarters, 10th Mountain Division	Fort Drum, NY
LTC (b) (6), (b) (7)	Ops Group C, Battle Command Training Program	Fort Leavenworth, Kansas
LTC (b) (6), (b) (7)(C)	Headquarters, 2d Brigade Combat Team, 10th Mountain Division	Fort Drum, NY
LTC (b) (6), (b) (7)(C)	1st Information Operations Command (Land)	Fort Belvoir, VA
LTC (b) (6), (b) (7)(C)	Headquarters, 1st Armored Division	Wiesbaden, Germany
LTC (b) (6), (b) (7)	US Army ROTC Instructor Group, Old Dominion University	Norfolk, VA
LTC (b) (6), (b) (7)	113th Medical Company (Combat Stress Control)	Stanton, CA
LTC (b) (6), (b) (7)(C)	Headquarters, 1st Armored Division	Wiesbaden, Germany
LTC (b) (6), (b) (7)(C)	J6, United States Forces-Iraq	Baghdad, Iraq
MAJ (b) (6), (b) (7)(C)	743d Military Intelligence Battalion	Buckley AFB, CO
MAJ (b) (6), (b) (7)	1st Information Operations Command (Land)	Fort Belvoir, VA
MAJ (b) (6), (b) (7)	Company C, 442d Signal Battalion	Fort Gordon, GA
MAJ (b) (6), (b)	Headquarters, 1st Armored Division	Wiesbaden, Germany
MAJ (b) (6), (b) (7)(C)	5th Signal Command	Mannheim, Germany
CPT (b) (6), (b) (7)(C)	Headquarters, 22d Chemical Battalion (Technical Escort)	Aberdeen Proving Grounds, MD
CPT (b) (6), (b) (7)(C)	Headquarters, 2d Brigade Combat Team, 10th Mountain Division	Fort Drum, NY
CPT (b) (6), (b) (7)(C)	Headquarters, 2d Brigade Combat Team, 10th Mountain Division	Fort Drum, NY
CPT (b) (6), (b) (7)(C)	Headquarters and Headquarters Company, 2d Brigade Special Troops Battalion, 10th Mountain Division	Fort Drum, NY
CPT (b) (6), (b) (7)(C)	Company A (MICCC), 304th Military Intelligence Battalion	Fort Huachuca, AZ

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

Individual	Organization	Location
CPT (b) (6), (b) (7)(C)	Headquarters, 4th Battalion, 31st Infantry	Fort Drum, NY
CPT	Kenner Army Health Clinic	Fort Lee, VA
CPT	Headquarters, First Army Division-East	Fort Meade, MD
CPT	Headquarters, 2d Brigade Combat Team, 10th Mountain Division	Fort Drum, NY
CPT	1908th Medical Detachment (Combat Stress Control)	Topeka, KS
1LT	Headquarters, 2d Brigade Combat Team, 10th Mountain Division	Fort Drum, NY
1LT (b) (6), (b) (7)(C)	Battery G (FSC), 3d Battalion, 82d Field Artillery	Fort Hood, TX
1LT	Headquarters, 2d Brigade Combat Team, 10th Mountain Division	Fort Drum, NY
1LT (b) (6), (b) (7)	Headquarters, 2d Brigade Combat Team, 10th Mountain Division	Fort Drum, NY
CW2 (b) (6), (b) (7)	Headquarters, 2d Brigade Combat Team, 10th Mountain Division	Fort Drum, NY
CW2 (b) (6), (b) (7)(C)	Headquarters, 2d Brigade Combat Team, 10th Mountain Division	Fort Drum, NY
CW2	Headquarters, 2d Brigade Combat Team, 10th Mountain Division	Fort Drum, NY
CW2	Headquarters, 19th Expeditionary Sustainment Command	US Army Garrison Henry, Korea
CW2 (b) (6), (b) (7)(C)	Company B, 741st Military Intelligence Battalion	Fort Meade, MD
WO1 (b) (6), (b) (7)	Headquarters, 2d Brigade Combat Team, 10th Mountain Division	Fort Drum, NY
CSM (b) (6), (b) (7)(C)	Headquarters, 1st Squadron, 89th Cavalry	Fort Drum, NY
MSG	Headquarters, 2d Brigade Combat Team, 10th Mountain Division	Fort Drum, NY
MSG (b) (6), (b) (7)	Headquarters, 2d Brigade Combat Team, 10th Mountain Division	Fort Drum, NY
MSG (b) (6), (b) (7)	Headquarters, 2d Brigade Combat Team, 10th Mountain Division	Fort Drum, NY
SFC (b) (6), (b) (7)(C)	Headquarters, 4th Infantry Division	Fort Carson, CO
SFC	Company B, 2d Brigade Special Troops Battalion, 10th Mountain Division	Fort Drum, NY
SFC (b) (6), (b) (7)(C)	Headquarters, 2d Brigade Combat Team, 4th Infantry Division	Fort Carson, CO
SFC (b) (6), (b) (7)(C)	US Army Element, US Strategic Command	Offutt AFB, NE
SFC (b) (6), (b) (7)	(US Army Retired)	

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

Individual	Organization	Location
SSG (b) (6), (b) (7)(C)	Headquarters, 10th Mountain Division and Fort Drum	Fort Drum, NY
SSG (b) (6), (b) (7)(C)	Headquarters, 2d Brigade Combat Team, 10th Mountain Division	Fort Drum, NY
PO1 (b) (6), (b) (7)	Center for Information Dominance, Corry Station	Naval Air Station Pensacola, FL
SSG (b) (6), (b) (7)(C)	Company B, 2/10 Brigade Special Troops Battalion	Fort Drum, NY
SSG	Company B, 2/10 Brigade Special Troops Battalion	Fort Drum, NY
SSG	Headquarters, 1st Armored Division	Wiesbaden, Germany
SSG (b) (6), (b)	Headquarters, 2d Brigade Combat Team, 10th Mountain Division	Fort Drum, NY
SSG (b) (6), (b) (7)	Headquarters, 2d Brigade Combat Team, 10th Mountain Division	Fort Drum, NY
SSG (b) (6), (b) (7)(C)	Company C, 741st Military Intelligence Battalion	Fort Meade, MD
SGT	Headquarters, 2d Brigade Combat Team, 10th Mountain Division	Fort Drum, NY
SGT (b) (6), (b) (7)(C)	Company B, 2/10 Brigade Special Troops Battalion	Fort Drum, NY
SGT	Company B, 2/10 Brigade Special Troops Battalion	Fort Drum, NY
SGT	Company B, 2/10 Brigade Special Troops Battalion	Fort Drum, NY
SGT	Headquarters, 2d Brigade Combat Team, 10th Mountain Division	Fort Drum, NY
SGT (b) (6), (b) (7)(C)	Company C, 229th Military Intelligence Battalion	Presidio of Monterey, CA
SGT (b) (6), (b) (7)(C)	Company B, 2/10 Brigade Special Troops Battalion	Fort Drum, NY
SGT	HHC, 2/10 Brigade Special Troops Battalion	Fort Drum, NY
SPC	HHC, 2/10 Brigade Special Troops Battalion	Fort Drum, NY
SPC	Headquarters, 2d Brigade Combat Team, 10th Mountain Division	Fort Drum, NY
SPC (b) (6), (b) (7)(C)	Headquarters, 3d Brigade Combat Team, 82d Airborne Division	Fort Bragg, NC
SPC (b) (6), (b) (7)	Company B, 3d Military Intelligence Battalion	US Army Garrison Humphreys, Korea
SPC (b) (6), (b) (7)(C)	Headquarters, 2d Brigade Combat Team, 10th Mountain Division	Fort Drum, NY
SPC (b) (6), (b) (7)(C)	(No longer in U.S. Army)	
SPC (b) (6), (b) (7)(C)	Headquarters, 2d Brigade Combat Team, 10th Mountain Division	Fort Drum, NY
SPC (b) (6), (b) (7)	Headquarters, 2d Brigade Combat Team, 10th Mountain Division	Fort Drum, NY

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

Individual	Organization	Location
SPC (b) (6), (b) (7)(C)	(No longer in U.S. Army)	
SPC	Headquarters, 2d Brigade Combat Team, 10th Mountain Division	Fort Drum, NY
SPC (b) (6), (b) (7)(C)	HHC, 2/10 Brigade Special Troops Battalion	Fort Drum, NY
SPC	Headquarters, 2d Brigade Combat Team, 10th Mountain Division	Fort Drum, NY
PFC (b) (6), (b) (7)(C)	Headquarters, 2d Brigade Combat Team, 10th Mountain Division	Fort Drum, NY
PFC (b) (6), (b) (7)(C)	Headquarters, 2d Brigade Combat Team, 10th Mountain Division	Fort Drum, NY
Ms. (b) (6), (b) (7)(C)	Headquarters, 10th Mountain Division and Fort Drum	Fort Drum, NY
Mr. Mayfield, David	Office of The Judge Advocate General	Washington, DC
Mr. (b) (6), (b) (7)(C)	General Dynamics Information Technology, Inc.	Fort Huachuca, AZ
Dr. Sageman, Marc	HQDA, Office of the Deputy Chief of Staff, G-2	Washington, DC
Mr. (b) (6), (b) (7)(C)	National Geospatial Intelligence Agency	Bethesda, MD
Mr. (b) (6), (b) (7)(C)	Headquarters, 10th Mountain Division and Fort Drum	Fort Drum, NY

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

Appendix 2: Investigative Team Members

LTG Robert L. Caslen, Jr.	OIC, Investigative Team	Combined Arms Center
LTC (b) (6), (b) (7)(C)	Deputy, Investigative Team	Combined Arms Center
COL (b) (6), (b) (7)(C)	Legal Advisor	Office of the Judge Advocate General
CPT (b) (6), (b) (7)(C)	Legal Advisor	Office of the Judge Advocate General
MG Michael T. Flynn	Investigative Officer	HQs, Dept. of the Army, G-2
COL (b) (6), (b) (7)(C)	Investigative Officer	Signal Center of Excellence
COL (b) (6), (b) (7)	Investigative Officer	Signal Center of Excellence
LTC (b) (6), (b) (7)(C)	Investigative Officer	Combined Arms Center
LTC (b) (6), (b) (7)(C)	Investigative Officer	Combined Arms Center
LTC (b) (6), (b) (7)(C)	Investigative Officer	Combined Arms Center
LTC (b) (6), (b) (7)(C)	Investigative Officer	Combined Arms Center
MAJ (b) (6), (b) (7)(C)	Investigative Officer	Combined Arms Center
CW4 (b) (6), (b) (7)(C)	Investigative Officer	Intelligence Center of Excellence
Mr. (b) (6), (b) (7)(C)	Investigative Officer	Signal Center of Excellence

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

Appendix 3: Abbreviations/Acronyms

ABN	Airborne
AD	Armored Division
AIT	Advanced Individual Training
ALARACT	All Army Activities
AOR	Area of Responsibility
APFT	Army Physical Fitness Test
AR	Army Regulation
ASVAB	Armed Services Vocational Aptitude Battery
BBP	Best Business Practices
BCT	Brigade Combat Team
C&A	Certification and Accreditation
CCF	Central Clearance Facility
CCHQ	CENTCOM Headquarters
CCR	CENTCOM Regulation
CD	Cavalry Division
CENTCOM	U.S. Central Command
CFH	CENTCOM Forward Headquarters
CFR	Code of Federal Regulations
CH	Chaplain
CID	U.S. Army Criminal Investigation Command
CIS	Chief of Information Systems
CND	Computer Network Defense
CNSSI	Committee on National Security Systems Instruction
CoC	Chain of Command
COP	Combat Outpost
COS	Contingency Operating Site
COTS	Commercial Off-the-Shelf
DA	Department of the Army
DAA	Designated Approving Authority or Designated Accreditation Authority
DCID	Director of Central Intelligence Directive
DCS	Deputy Chief of Staff
DEROG	Report of Unfavorable Information for Security Determination (DA Form 5248-R)
DIA	Defense Intelligence Agency
DIACAP	DoD Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DISN	Defense Information Systems
DITSCAP	Defense Information Technology Certification and Accreditation Process
DNI	Director of National Intelligence
DNS	Domain Name Server

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoDIIS	Department of Defense Intelligence Information System
DoJ	Department of Justice
DTM	Directive-Type Memorandum
e-QIP	Electronic Questionnaire for Investigations Processing
ERB	Enlisted Records Brief
EXORD	Execution Order
FM	Field Manual
FORSCOM	U.S. Army Forces Command
FTR	Failure to Repair
G-2	General Staff Intelligence Section
G-6	General Staff Signal Section
GOMOR	General Officer Memorandum of Reprimand
GOTS	Government Off-the-Shelf
HBSS	Host-Based Security System
HHC	Headquarters and Headquarters Company
HIPAA	Health Insurance Portability and Accountability Act
HP/RR/SP	Health Promotion/ Risk Reduction/Suicide Prevention
HQDA	Headquarters, Department of the Army
HUMINT	Human Intelligence
IA	Information Assurance
IAM	Information Assurance Manager
IANE	Information Assurance Network Engineer
IANM	Information Assurance Network Manager
IASO	Information Assurance Security Officer
IAT	Information Assurance Technician
IAVM	Information Assurance Vulnerability Management
IC	Intelligence Community
ICD	Intelligence Community Directive
IJOA	Iraq Joint Operating Area
ILE	Intermediate Level Education
INFOSEC	Information Security
IRTF	Information Review Task Force
IS	Information System
ISSO	Information System Security Officer
IT	Information Technology
JFCOM	U.S. Joint Forces Command
JP	Joint Publication
JRE	Joint Reform Effort
JSS	Joint Security Station

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

JTF	Joint Task Force
MEDCOM	Medical Command
MFR	Memorandum For record
MND-B	Multi-National Division-Baghdad
MNF-I	Multi-National Forces-Iraq
MOS	Military Occupational Specialty
MSC	Major Subordinate Command
MTN	Mountain
NCIC	National Crime Information Center
NCOES	Noncommissioned Officer Education System
NCOIC	Noncommissioned Officer-In-Charge
NEC	Network Enterprise Center
NETCOM	US Army Network Enterprise Technology Command
NIPRNET	Nonsecure Internet Protocol Router Network
NIS	National Investigative Standards
NIST	National Institute of Standards
NSTISSI	National Security Telecommunications and Information Systems Security Committee Instruction
OIC	Officer in-Charge
OPM	Office of Personnel Management
OTSG	Office of the Surgeon General
PHI	Personal Health Information
PII	Personally Identifiable Information
PL	Public Law
POA&M	IT Security Plan of Action and Milestones
PT	Physical Training
RCERT	Regional Computer Emergency Response Team
RIP/TOA	Relief in Place/Transfer of Authority
S-2	Brigade/Battalion Intelligence Section
S-6	Brigade/Battalion Signal Section
SA	Special Agent
SAV	Staff Assistance Visit
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SF	Standard Form
SIGACT	Significant Activity
SIGINT	Signals Intelligence
SIO	Senior Intelligence Official or Senior Intelligence Officer
SIPRNET	Secure Internet Protocol Router Network
SSBI	Single Scope Background Investigation
SSO	Special Security Officer
SSR	Special Security Representative

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

ST	Skilled/Technical (ASVAB category)
STT	Stability Transition Team
TASO	Terminal Automation Security Officer
TNOSC	Theater Network Operations and Security Center
TPI	Two-Person Integrity
TS	Top Secret
UCMJ	Uniformed Code of Military Justice
UK	United Kingdom
USC	United States Code
USD-C	United States Division-Center
USF-I	United States Forces-Iraq
XO	Executive Officer

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

Appendix 4: Abbreviations of Ranks

Enlisted/Noncommissioned officers

PVT	Private
PFC	Private First Class
SPC	Specialist
SGT	Sergeant
SSG	Staff Sergeant
SFC	Sergeant First Class
MSG	Master Sergeant
1SG	First Sergeant
SGM	Sergeant Major
CSM	Command Sergeant Major

Warrant Officers

WO1	Warrant Officer One
CW2	Chief Warrant Officer Two
CW3	Chief Warrant Officer Three
CW4	Chief Warrant Officer Four

Commissioned Officers

2LT	Second Lieutenant
1LT	First Lieutenant
CPT	Captain
MAJ	Major
LTC	Lieutenant Colonel
COL	Colonel
BG	Brigadier General
MG	Major General
LTG	Lieutenant General

Naval Officers

LTJG	Lieutenant, Junior Grade
LT	Lieutenant
LCDR	Lieutenant Commander
CDR	Commander
CAPT	Captain
RDML	Rear Admiral (Lower Half)

Appendix 5: Definitions

Access control
The process of granting or denying specific requests: 1) for obtaining and using information and related information processing services; and 2) to enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances). (CNSSI 4009)

Accreditation
(USG) Formal declaration by a Designated Accrediting Authority (DAA) or Principal Accrediting Authority (PAA) that an information system is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards. (CNSSI 4009)

Accreditation Decision
(Army) An official designation from a DAA, in writing or digitally signed Email, made visible to the CIO/G–6, regarding acceptance of the risk associated with operating an IS. Expressed as ATO, IATO, IATT, or DATO.

Authentication
(USG) The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data. (CNSSI 4009)

Authorization to operate (ATO)
(DoD) Authorization granted by a DAA for a DoD IS to process, store, or transmit information. An ATO indicates a DoD IS has adequately implemented all assigned IA controls to the point where residual risk is acceptable to the DAA. ATOs may be issued for up to 3 years. (DoDI 8510.01)

Availability
(USG) The property of being accessible and useable upon demand by an authorized entity. (CNSSI 4009)

Bandwidth
(Army) The maximum rate at which an amount of data can be sent through a given transmission channel. (AR 25-1)

Certification
(USG) Comprehensive evaluation of the technical and non-technical security features of an IS and other safeguards, made in support of the accreditation process, to establish

the extent to which a particular design and implementation meets a set of specified security requirements. (CNSSI 4009)

Certification and accreditation
The standard DoD approach for identifying information security requirements, providing security solutions, and managing the security of DoD information systems. (AR 25-2)

Collateral
(DoD) All national security information classified Confidential, Secret, or Top Secret under the provisions of an Executive order for which special systems of compartmentation (such as SCI or SAPs) are not formally required. (DoDI 5200.01)

Computer Network Defense (CND)
(DoD) Actions taken to protect, monitor, analyze, detect and respond to unauthorized activity within Department of Defense information systems and computer networks. Also called CND. (JP 1-02)

Computing environment
(USG) Workstation or server (host) and its operating system, peripherals, and applications. (CNSSI 4009)

Confidentiality
(USG) The property that information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information. (CNSSI 4009)

Denial of authorization to operate (DATO)
(USG) DAA determination that an information system cannot operate because of an inadequate IA design or failure to implement assigned IA controls. If the system is already in use, operation of the system is halted. (CNSSI 4009)

Designated approving authority (DAA)
(USG) Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with authorizing official, designated accrediting authority, and delegated accrediting authority. (CNSSI 4009)

(Army) A general officer (GO), SES or equivalent official appointed by the Army CIO/G–6 with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with Designated Authorization Authority and Delegated Accrediting Authority. (AR 25-2)

DIACAP Package
(DoD) The collection of documents or collection of data objects generated through DIACAP implementation for an IS. A DIACAP package is developed through implementing the activities of the DIACAP and maintained throughout a system's life cycle. Information from the package is made available as needed to support an accreditation or other decision such as a connection approval. (DoDI 8510.01)

DoD Information Assurance Certification and Accreditation Process (DIACAP)
(DoD) The DoD process for identifying, implementing, validating, certifying, and managing IA capabilities and services, expressed as IA controls, and authorizing the operation of DoD ISs, including testing in a live environment, in accordance with statutory, Federal, and DoD requirements. (DoDI 8510.01)

Domain
(USG) An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture. See also security domain. (CNSSI 4009)

Enclave
(USG) Collection of information systems connected by one or more internal networks under the control of a single authority and security policy. The systems may be structured by physical proximity or by function, independent of location. (CNSSI 4009)

(DoD) Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves always assume the highest mission assurance category and security classification of the AIS applications or outsourced IT-based processes they support, and derive their security needs from those systems. They provide standard IA capabilities, such as boundary defense, incident detection and response, and key management, and also deliver common applications, such as office automation and electronic mail. Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers. (DoDI 8500.02)

End-to-end security
(USG) Safeguarding information in an information system from point of origin to point of destination. (CNSSI 4009)

Host Based Security System (HBSS)
The HBSS baseline is a flexible, commercial off-the-shelf (COTS) based application. The system can detect and counter, in real-time, against known cyber-threats to Department of Defense (DoD) enterprise. Under the sponsorship of the Enterprise-wide Information Assurance and Computer Network Defense Solutions Steering Group (ESSG), the HBSS solution will be attached to each host (server, desktop, and laptop) in DoD. The system will be managed by local administrators and configured to block known-bad traffic using an Intrusion Prevention System (IPS) and host firewall. (DISA)

Identity-based access control
(USG) Access control based on the identity of the user (typically relayed as a characteristic of the process acting on behalf of that user) where access authorizations to specific objects are assigned based on user identity. (CNSSI 4009)

Information Assurance (IA)
(DoD) Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (DoDD 8500.01E, 24 OCT 02) (JP 1-02)

(Army) The protection of systems and information in storage, processing, or transit from unauthorized access or modification; denial of service to unauthorized users; or the provision of service to authorized users. It also includes those measures necessary to detect, document, and counter such threats. Measures that protect and defend information and ISs by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of ISs by incorporating protection, detection, and reaction capabilities. This regulation designates IA as the security discipline that encompasses COMSEC, INFOSEC, and control of compromising emanations (TEMPEST). (AR 25-2)

Information Assurance Manager (IAM)
(USG) Individual responsible for the information assurance of a program, organization, system, or enclave. Listed under Information Systems Security Manager (ISSM) (CNSSI 4009)

Information Assurance Officer (IAO)
(DoD) An individual responsible to the IAM for ensuring that the appropriate operational IA posture is maintained for a DoD information system or organization. While the term IAO is favored within the Department of Defense, it may be used interchangeably with other IA titles (e.g., Information Systems Security Officer, Information Systems Security Custodian, Network Security Officer, or Terminal Area Security Officer). (DoDI 8500.02)

Information Assurance Vulnerability Management (IAVM)
IAVM is the DoD program to identify and resolve identified vulnerabilities in operating systems. It requires the completion of four distinct phases to ensure compliance.

Information Security (INFOSEC)
(DoD) The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. (JP 1-02)

(DoD) The system of policies, procedures, and requirements established under the authority of E.O. 12958 (reference (e)) to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security. (DoD 5200.01-R)

Information Systems Security Officer (ISSO)
(USG) Individual assigned responsibility for maintaining the appropriate operational security posture for an information system or program. (CNSSI 4009)

Information Technology (IT)
(USG) (Army) Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used directly or is used by a contractor under a contract with the executive agency which 1) requires the use of such equipment, or 2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" also includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. The term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. (AR 25-1) (40 U.S.C. 1401 et seq.)

Inside(r) threat
(USG) An entity with authorized access (i.e., within the security domain) that has the potential to harm an information system or enterprise through destruction, disclosure, modification of data, and/or denial of service. (CNSSI 4009)

Integrity
(USG) The property whereby an entity has not been modified in an unauthorized manner. (CNSSI 4009)

(NIST) Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. (NIST 800-53).

Intelligence Community (IC) and elements of the Intelligence Community.
(USG) Consistent with section 3.5(h) of Executive Order 12333, as amended, the Office of the Director of National Intelligence; the Central Intelligence Agency; the National Security Agency; the Defense Intelligence Agency; the National Geospatial Intelligence Agency; the National Reconnaissance Office; other offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs; the intelligence and counterintelligence elements of the Army, the Navy, the Air Force, and the Marine Corps; the intelligence elements of the Federal Bureau of Investigation; the Office of National Security Intelligence of the Drug Enforcement Administration; the Office of Intelligence and Counterintelligence of the Department of Energy; the Bureau of Intelligence and Research of the Department of State; the Offices of Intelligence and Analysis of the Department of the Treasury and the Department of Homeland Security; the intelligence and counterintelligence elements of the Coast Guard; and such other elements of any department or agency as may be designated by the President, or designated jointly by the Director and the head of the department or agency concerned, as an element of the Intelligence Community. (DoDI 5200.01)

Interim authority to operate (IATO)
(USG) Temporary authorization granted by the DAA to operate an information system under the conditions or constraints enumerated in the Accreditation Decision. (CNSSI 4009)

Interim authority to test (certification and accreditation) (IATT)
(USG) Temporary authorization granted by the DAA to test an information system in a specified operational information environment (usually a live information environment or with live data) within the timeframe and under the conditions or constraints enumerated in the Accreditation Decision. (CNSSI 4009)

IT Position Category
(DoD) Applicable to unclassified DoD information systems, a designator that indicates the level of IT access required to execute the responsibilities of the position based on the potential for an individual assigned to the position to adversely impact DoD missions or functions. Position categories include: IT-I (Privileged), IT-II (Limited Privileged) and IT-III (Non-Privileged), as defined in reference (o). Investigative requirements for each category vary, depending on role and whether the incumbent is a U.S. military member, U.S. civilian government employee, U.S. civilian contractor or a foreign national. The term IT Position is synonymous with the older term Automated Data Processing (ADP) Position. (DoDD 8500.01E)

IT Security Plan of Action and Milestones (POA&M)
(DoD) A permanent record that identifies tasks to be accomplished in order to resolve security weaknesses. Required for any accreditation decision that requires corrective actions, it specifies resources required to accomplish the tasks enumerated in the plan and milestones for completing the tasks. Also used to document DAA-accepted non-compliant IA controls and baseline IA controls that are not applicable. An IT Security POA&M may be active or inactive throughout a system's life cycle as weaknesses are newly identified or closed. (DoDI 8510.01)

Need-to-know
(USG) A method of isolating information resources based on a user's need to have access to that resource in order to perform their job but no more. The terms 'need-to know" and "least privilege" express the same idea. Need-to-know is generally applied to people, while least privilege is generally applied to processes. (CNSSI 4009)

(Army) Approved access to, or knowledge or possession of, specific information required to carry out official duties. (AR 25-2)

Network
(Army) Communications medium and all components attached to that medium whose function is the transfer of information. Components may include ISs, packet switches, telecommunications controllers, key distribution centers, and technical control devices. (AR 25-2)

Network security
(USG) See information assurance. (CNSSI 4009)

(Army) Protection of networks and their services from unauthorized modification, destruction, or disclosure. It provides assurance the network performs its critical functions correctly and there are no harmful side effects. (AR 25-2)

Non-privileged access
(Army) User-level access; normal access given to a typical user. Generally, all access to system resources is controlled in a way that does not permit those controls and rules to be changed or bypassed by a typical user. (AR 25-2)

Non-repudiation
(USG) Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information. (CNSSI 4009)

(NIST) Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message. (NIST 800-53)

Personally Identifiable Information (PII)
(USG) Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. (CNSSI 4009)

Plan of Action and Milestones (POA&M)
See IT Security Plan of Action and Milestones (POA&M).

Principle of least privilege
(Army) The principle of least privilege requires that a user be given no more privilege than necessary to perform a job. Ensuring least privilege requires identifying what the user's job is, determining the minimum set of privileges required to perform that job, and restricting the user to a system or domain with those privileges and nothing more. (AR 25-2)

Privileged access
(Army) Authorized access that provides a capability to alter the properties, behavior, or control of the information system or network. It includes, but is not limited to, any of the following types of access:

a. "Super user," "root," or equivalent access, such as access to the control functions of the information system or network, administration of user accounts, and so forth.

b. Access to change control parameters (for example, routing tables, path priorities, addresses) of routers, multiplexers, and other key information system or network equipment or software.

c. Ability and authority to control and change program files, and other users' access to data.

d. Direct access (also called unmediated access) to functions at the operating-system level that would permit system controls to be bypassed or changed.\

e. Access and authority for installing, configuring, monitoring, or troubleshooting the security monitoring functions of information systems or networks (for example, network or system analyzers; intrusion detection software; firewalls) or in performance of cyber or network defense operations. (AR 25-2)

Role-Based Access Control (RBAC)
(USG) Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals. (CNSSI 4009)

Senior Intelligence Official (SIO)
(USG) The highest ranking military or civilian official charged with direct foreign intelligence missions, functions, or responsibilities within a department, agency, component, or element of an Intelligence Community organization. (DoDI 5200.01) Also synonymous with Senior Intelligence Officer.

Sensitive Compartmented Information (SCI)
(DoD) All information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentation have been or will be formally established. (These controls are over and above the provisions of DoD 5200.1-R, Information Security Program Regulation.) Also called SCI. (JP 1-02)

Sensitive Compartmented Information Facility (SCIF)
(DoD) An accredited area, room, group of rooms, or installation where sensitive compartmented information (SCI) may be stored, used, discussed, and/or electronically processed. Sensitive compartmented information facility (SCIF) procedural and physical measures prevent the free access of persons unless they have been formally indoctrinated for the particular SCI authorized for use or storage within the SCIF. Also called SCIF. See also sensitive compartmented information. (JP 1-02)

Sensitive information
(USG) Any information the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under 5 USC 552a (The Privacy Act), but which has not been specifically authorized under criteria established by executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. Sensitive information includes information in routine DoD payroll, finance, logistics, and personnel management systems. Examples of sensitive information include, but are not limited to, the following categories:

a. FOUO, in accordance with DoD 5400.7–R, is information that may be withheld from mandatory public disclosure under the FOIA.

b. Unclassified technical data is data related to military or dual-use technology that is subject to approval, licenses, or authorization under the Arms Export Control Act and withheld from public disclosure in accordance with DoD 5230.25.

c. Department of State (DOS) sensitive but unclassified (SBU) is information originating from the DOS that has been determined to be SBU under appropriate DOS information security policies.

d. Foreign government information is information originating from a foreign government that is not classified CONFIDENTIAL or higher but must be protected in accordance with DoD 5200.1–R.

e. Privacy data is personal and private information (for example, individual medical information, home address and telephone number, social security number) as defined in the Privacy Act of 1974. (AR 25-2)

System administrator (SA)
(USG) A system administrator (SA), or "sysadmin," is a privileged-level individual employed or authorized to maintain and operate a computer system or network. Individual responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established information assurance policy and procedures. (CNSSI 4009)

TEMPEST
(USG) A name referring to the investigation, study, and control of compromising emanations from telecommunications and automated information systems equipment. (CNSSI 4009)

(DoD) An unclassified term referring to technical investigations for compromising emanations from electrically operated information processing equipment; these investigations are conducted in support of emanations and emissions security. (JP 1-02)

Thin client
(Army) The use of client-server architecture networks which depends primarily on the central server for processing activities which focuses on conveying input and output between the user and the remote server. In contrast, a thick or fat client does as much processing as possible and passes only data for communications and storage to the server. Many thin client devices run only web browsers or remote desktop software, meaning that all significant processing occurs on the server. (AR 25-1)

Two-Person Control (TPC)
(USG) Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and unauthorized procedures with respect to the task being performed and each familiar with established security and safety requirements. (CNSSI 4009)

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

Two-Person Integrity (TPI)
(USG) System of storage and handling designed to prohibit individual access by requiring the presence of at least two authorized individuals, each capable of detecting incorrect or unauthorized security procedures with respect to the task being performed. (CNSSI 4009)

Wide area network (WAN)
(Army) A WAN covers a wider geographic area than a LAN, is an integrated voice or data network, often uses common carrier lines for the interconnection of its LANs, and consists of nodes connected over point-to-point channels. Commercial examples are Internet and public data. Government examples are NIPRNET and SIPRNET. (AR 25-2)

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

Appendix 6: References

Committee on National Security Systems Instruction (CNSSI) No. 4009, *National Information Assurance Glossary.*

Director of Central Intelligence Directive 6/3, *Protecting Sensitive Compartmented Information Within Information Systems Manual,* June 1999.
DoD Manual 5105.21-M-1, "Department of Defense Sensitive Compartmented Information Administrative Security Manual," August 1998
DoD Instruction 5200.1, *DoD Information Security Program and Protection of Sensitive Compartmented Information*, October 9, 2008
DoD Manual 5200.1-R, *Information Security Program*, January 1997
DoD Regulation 6025.18-R, DoD Health Information Policy Regulation, January 24, 2003
DoD Directive 8500.1, *Information Assurance,* October 24, 2002.
DoD Instruction 8500.2, *Information Assurance Implementation*, February 6, 2003.
DoD Instruction 8510.01 *DoD Information Assurance Certification and Accreditation Process (DIACAP),* November 28, 2007
DoD Directive 8570.01, *Information Assurance Training, Certification, and Workforce Management,* August 14, 2004
DoD Manual 8570.01-M, *Information Assurance Workforce Improvement Program* (Incorporating Change 2), April 20, 2010

Department of Defense Task Force on Mental Health Report, "An Achievable Vision: Report of the Department of Defense Task Force on Mental Health Final Report", June 2007

CJCS Instruction 6510.01E, *Information Assurance (IA) and Computer Network Defense (CND),* August 2007

Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms,* 8 November 2010 (As Amended Through 31 December 2010)

USCENTCOM Regulation 10-3, *Terms of Reference for Component Commanders and Other Organizations in the USCENTCOM Area of Responsibility*, June 2010
USCENTCOM Regulation 25-200, *Information Resources Management,* August 2009
USCENTCOM Regulation 25-206, *Network Operations (NetOps)*, October 2007
USCENTCOM Regulation 380-1, *Information Security Program Regulation*, April 2007
USCENTCOM Regulation 380-3, *Sensitive Compartmented Information (SCI) Access*, October 2008
USCENTCOM Regulation 380-12, *Sensitive Compartmented Information (SCI) Security Management* (obsolete), August 1988

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

USCENTCOM Regulation 380-12, *Sensitive Compartmented Information (SCI) Security Management*, Aug 2010

AR 15-6, *Procedures for Investigating Officers and Boards of Officers*, 2 October 2006
AR 25-1, *Army Knowledge Management and Information Technology*, 4 December 2008
AR 25-2, *Information Assurance*, 24 October 2007
AR 27-10, *Legal Services, Military Justice* ,16 November 2005
AR 40-66, *Medical Record Administration and Health Care Documentation*, 17 June 2008
AR 190–13, *The Army Physical Security Program*, September 1993
AR 190–16, *Physical Security*, May 1991
AR 350-1, *Army Training and Leader Development*, 18 December 2009
AR 380-5, *Department of the Army Information Security Program*, 29 September 2000
AR 380–53, *Information Systems Security Monitoring*, April 1998
AR 380-67, *The Department of the Army Personnel Security Program*, 9 September 1988
AR 381-12, *Threat Awareness and Reporting Program*, 4 October 2010
AR 600-20, *Army Command Policy*, 18 Mar 08, with Rapid Action Revision 003, 27 April 2010
AR 635-200, *Active Duty Enlisted Administrative Separations*, 6 Jun 2005

ALARACT 245/2010, Sensitive Information in the Public Domain, DTG: P 141042ZAUG10 (Corrected Copy)
ALARACT 246/2010, Application of Information Security Procedures, DTG: 170133ZAUG 10
ALARACT 256-2010, Directed Actions to Safeguard Against Unauthorized Information Dissemination, DTG: P 211048Z AUG10 (U)
ALARACT 260-2010, HQDA EXORD 307-10 ISO WikiLeak Actions to Be Taken by the ACOM, ASCC, DRU, and Army Staff, DTG: P 260029ZAUG10

Field Manual 6-02.71, Network Operations, July 14, 2009

Multi-National Force-Iraq Directive 25-1, *Information Assurance Implementation*, 2007

United States Forces-Iraq Directive 25-1, *Information Assurance Implementation*, 2010

United States Division-Center Policy Letter 6-1, *Information Assurance/ Computer Network Defense Policy and Procedures*, January 13, 2010

US Army Medical Command Regulation 40-38, *Command Directed Mental Health Evaluations*, June 1, 1999

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

US Army Network Enterprise Technology Command, "Information Assurance Training Best Business Practices," February 28, 2006, updated July 26, 2010, corrected copy August 6, 2010

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

Appendix 7:
Table of Contents (Long Form) / Detailed Exhibit Listing

Tab A	**DA Form 1574 and AR 15-6 IO Memorandum Re: Findings and Recommendations**
Tab B	**Legal Review**
Tab C	**Appointment Memoranda**
C1	SECDEF Memorandum to SECARMY Directing Wikileaks 15-6 (14 Dec 10)
C2	SECARMY Memorandum of Appointment Appointing LTG Robert L. Caslen, Jr. as 15-6 Investigating Officer (16 Dec 10)
Tab D	**Appointing Official's Instructions and Investigative Methodology**
Tab E	**Witness Statements and Memoranda Re: Witness Interviews**
E1	(b) (6), (MSG (b) (6), (b) (7)(C))
E1-1	▪ MFR Re: PFC Manning, "SUBJECT: Behaviour of SPC Bradley Manning" (Signed) (2 Pages) (Typed), 21 Dec 09
E1-2	▪ MFR Re: PFC Manning, "SUBJECT: Recent Behaviour of SPC Bradley Manning"(Unsigned) (2 Pages) (Typed), 26 Apr 10 (Misdated 26 Apr 09)
E1-3	▪ MFR Re: PFC Manning, "SUBJECT: Recent Behaviour of SPC Bradley Manning" (Signed) (2 Pages) (Typed), 08 May 10
E1-4	▪ Email June 03, 2010 (with Photo) (Email obtained from CPT (b) (7)(C), (b) (3 Pages; 2 Email, 1 Photo)
E1-5	▪ DA Form 2823, Sworn Stmt (6 Pages) (Handwritten), 10 Jun 10
E1-6	INTENTIONALLY LEFT BLANK
E1-7	▪ DA Form 2823, Sworn Stmt (5 Pages) (Handwritten), 3 Jul 10
E1-8	INTENTIONALLY LEFT BLANK
E1-9	▪ DA Form 2823, Sworn Stmt (4 Pages) (Handwritten), 15 Jul 10
E1-10	▪ AIR (Agent's Investigation Report) (1 Page) (Typed)
E1-11	▪ DA FORM 3881, Rights Warning procedure/Wavier Certificate, MSG (b) (b)(6) 18 Jan 11
E2	(b) (6), (b) (7) (Mr (b) (6), (b) (7)(C))
E2-1	▪ Interview MFR (2 Pages) (Typed), 24 Jan 11
E3	(b) (6), (b) (7) (1LT (b) (6), (b) (7)(C))
E3-1	INTENTIONALLY LEFT BLANK
E3-2	▪ Canvass Interview Worksheet w/ Q&As, 11 Aug 10
E4	(b) (6), (SSG (b) (6), (b) (7)(C))
E4-1	▪ DA Form 2823, Sworn Stmt (2 Pages) (Typed), 6 Jan 11
E5	(b) (6), (2LT (b) (6), (b) (7)(C)),
E5-1	▪ DA Form 2823, Sworn Stmt (3 Pages) (Typed), 25 Aug 10
E6	(b) (6), (SPC (b) (6), (b) (7))
E6-1	▪ DA Form 2823, Sworn Stmt (3 Pages) (Handwritten), 28 May 10
E6-2	▪ DA Form 2823, Sworn Stmt (3 Pages) (Handwritten), 10 Jun 10

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

E7	[redacted] (PFC [redacted])
E7-1	▪ DA Form 2823, (ACICA) Sworn Stmt (3 Pages) (Typed), 8 May 10
E7-2	▪ DA Form 2823, (ACICA) Sworn Stmt (3 Pages) (Handwritten), 27 Jun 10
E7-3	INTENTIONALLY LEFT BLANK
E7-4	▪ DA Form 2823, (15-6) Sworn Stmt (2 Pages) (Typed), 19 Jan 11
E8	[redacted] (WO1 [redacted])
E8-1	▪ AIR (Agent's Investigation Report) (2 Pages) (Typed), 17 Dec 10
E8-2	▪ DA Form 2823, Sworn Stmt (5 Pages) (Typed) PLUS DA Form 3881, Rights Warning Procedure/Waiver Certificate, 18 Jan 11
E8-3	▪ Interview MFR (2 Pages) (Typed), 24 Jan 11
E8-4	▪ Interview MFR (1 Page) (Typed), 29 Jan 11
E9	[redacted] (SGT [redacted])
E9-1	▪ DA Form 2823, Sworn Stmt (3 Pages) (Typed), 18 Jan 11
E10	[redacted] (SGT [redacted])
E10-1	▪ DA Form 2823, Sworn Stmt (2 Pages) (Typed), 25 Aug 10
E11	[redacted] (SSG [redacted])
E11-1	▪ DA Form 2823, Sworn Stmt (2 Pages) (Handwritten), 28 May 10
E12	[redacted] (SGT [redacted])
E12-1	▪ DA Form 2823, Sworn Stmt (2 Pages) (Handwritten), 21 Jun 10
E13	[redacted] (CPT [redacted])
E13-1	▪ AIR (Agent's Investigation Report) (1 Page) (Typed), 25 May 10
E13-2	▪ DA Form 2823, Sworn Stmt (3 Pages) (Typed with Q&A Handwritten), 11 Jun 10
E13-3	▪ DA Form 2823, Sworn Stmt (2 Pages) (Typed), 14 Jul 10
E13-4	▪ AIR (Agent's Investigation Report) (2 Pages) (Typed), 5 Jan 11
E13-5	▪ DA Form 2823, Sworn Stmt (5 Pages) (Typed), 6 Jan 11
E13-6	▪ DA Form 2823, Sworn Stmt (2 Pages) (Typed), 21 Jan 11
E13-7	▪ Interview MFR (2 Pages) (Typed), 23 Jan 11
E14	[redacted] (SrA [redacted])
E14-1	▪ AIR (Agent's Investigation Report) (2 Pages) (Typed), 14 Sep 10
E15	[redacted] (MAJ [redacted])
E15-1	▪ Interview MFR (3 Pages) (Typed), interviewed 19 Jan 11, written 03 Feb 11
E16	[redacted] (SPC [redacted])
E16-1	▪ DA Form 2823, Sworn Stmt (4 Pages) (Handwritten), 21 Jun 10
E16-2	INTENTIONALLY LEFT BLANK
E16-3	▪ DA Form 2823, Sworn Stmt (2 Pages) (Typed), 19 Jan 11
E17	[redacted] (CPT [redacted])
E17-1	▪ DA Form 2823, Sworn Stmt (3 Pages) (Handwritten), 10 Jun 10
E17-2	▪ DA Form 2823, Sworn Stmt (2 Pages) (Typed), 18 Jan 11
E17-3	▪ Interview MFR (2 Pages) (Typed), 25 Jan 11

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

E18	[redacted] (SFC [redacted])
E18-1	▪ Canvass Interview Worksheet w/ Q&As, 11 Aug 10
E19	INTENTIONALLY LEFT BLANK
E20	[redacted] (LTC [redacted])
E20-1	▪ DA Form 2823, Sworn Stmt (2 Pages) (Typed), 6 Jan 11
E21	[redacted] (MAJ [redacted])
E21-1	▪ Interview MFR (2 Pages) (Typed), 24 Jan 11
E22	[redacted] (CSM [redacted])
E22-1	▪ DA Form 2823, Sworn Stmt (3 Pages) (Typed), 19 Jan 11
E23	[redacted] (MAJ [redacted])
E23-1	▪ DA Form 3881 (1 Page), 20 Jan 11
E23-2	▪ DA Form 2823 (2 Pages), 20 Jan 11
E24	[redacted] (SFC [redacted])
E24-1	▪ DA Form 2823, Sworn Stmt (2 Pages) (Typed), 25 Jul 10
E25	[redacted] (CW2 Chad [redacted]
E25-1	▪ Interview MFR (2 Pages) (Typed), 23 Jan 11
E26	[redacted] (CW2 [redacted])
E26-1	▪ DA Form 2823, Sworn Stmt (2 Pages) (Typed), 1 Oct 10
E26-2	▪ AIR (Agent's Investigation Report) (3 Pages) (Typed), 17 Dec 10
E26-3	▪ Interview MFR (3 Pages) (Typed), 20 Jan 11
E26-4	▪ Interview MFR (2 Pages) (Typed), 24 Jan 11
E26-5	▪ Interview MFR (2 Pages) (Typed), 02 Feb 11
E27	[redacted] (SFC [redacted])
E27-1	▪ DA Form 2823, Sworn Stmt (2 Pages) (Typed), 21 Jan 11
E28	[redacted] (1LT [redacted])
E28-1	▪ AIR (Agent's Investigation Report) (3 Pages) (Typed), 5 Jan 11
E28-2	▪ DA Form 2823, Sworn Stmt (3 Pages) (Typed), 18 Jan 11
E28-3	▪ DA Form 2823, Sworn Stmt (2 Pages) (Typed), 20 Jan 11
E29	[redacted] (PFC [redacted])
E29-1	▪ DA Form 2823, Sworn Stmt (2 Pages) (Typed), 22 Jun 10
E30	[redacted] (SGT [redacted])
E30-1	▪ Canvass Interview Worksheet w/ Q&As, 11 Aug 10
E31	[redacted] (PO1 [redacted])
E31-1	▪ AIR (Agent's Investigation Report) (2 Pages) (Typed), 20 Oct 10
E32	[redacted] (CPT [redacted])
E32-1	▪ DA Form 2823, Sworn Stmt (4 Pages) (Handwritten), 11 Jun 10
E32-2	▪ AIR (Agent's Investigation Report) (2 Pages) (Typed), 5 Jan 11
E32-3	▪ DA Form 2823, Sworn Stmt (4 Pages) (Typed), 7 Jan 11
E33	[redacted] (1LT [redacted])
E33-1	▪ DA Form 2823, Sworn Stmt (3 Pages) (Typed), 19 Jan 11
E34	[redacted] (LTC [redacted])

E34-1	▪ Interview MFR (3 Pages) (Typed), 23 Jan 11
E34-2	▪ Interview MFR (2 Pages) (Typed), 31 Jan 11
E35	INTENTIONALLY LEFT BLANK
E36	[redacted] (MAJ [redacted])
E36-1	▪ Interview MFR (2 Pages) (Typed), 23 Jan 11
E37	[redacted] (SPC [redacted])
E37-1	▪ DA Form 2823, Sworn Stmt (4 Pages) (Typed), 9 Sep 10
E38	[redacted] (SPC [redacted])
E38-1	▪ Canvass Interview Worksheet w/ Q&As, 11 Aug 10
E39	[redacted] (LTC [redacted])
E39-1	▪ Interview MFR (2 Pages) (Typed), 24 Jan 11
E40	[redacted] (Ms. [redacted])
E40-1	▪ DA Form 2823, Sworn Stmt (2 Pages) (Typed), 6 Jan 11
E41	[redacted] (SSG [redacted])
E41-1	▪ DA Form 2823, Sworn Stmt (3 Pages) (Typed), 7 Jan 11
E42	[redacted] (SGT [redacted])
E42-1	▪ Canvass Interview Worksheet w/ Q&As, 11 Aug 10
E43	[redacted] (CPT [redacted])
E43-1	▪ DA Form 2823, Sworn Stmt (3 Pages) (Typed), 21 Jan 11
E44	[redacted] (CPT [redacted])
E44-1	▪ AIR (Agent's Investigation Report) (2 Pages) (Typed), 6 Jan 11
E44-2	▪ DA Form 2823, Sworn Stmt (5 Pages) (Typed), 7 Jan 11
E45	[redacted] (LTC [redacted])
E45-1	▪ Interview MFR (6 Pages) (Typed), 10 Jan 11
E45-2	▪ Interview MFR (2 Pages) (Typed), 24 Jan 11
E46	[redacted] (CW2 [redacted])
E46-1	▪ DA Form 2823, Sworn Stmt (6 Pages) (Typed), 6 Jan 11
E47	[redacted] (CPT [redacted])
E47-1	▪ DA Form 2823, Sworn Stmt (3 Pages) (Handwritten), 10 Jun 10
E47-2	▪ DA Form 2823, Sworn Stmt (3 Pages) (Typed), 14 Jul 10
E47-3	▪ AIR (Agent's Investigation Report) (5 Pages) (Typed), 30 Dec 10
E47-4	▪ DA Form 2823, Sworn Stmt (6 Pages) (Typed), 13 Jan 11
E47-5	▪ DA Form 4856, Counseling Form (2 Pages) CPT [redacted] counsels MSG [redacted] regarding MSG [redacted] not forwarding PFC Manning's email that has the photo, 07 Jun 10
E48	[redacted] (CW2 [redacted])
E48-1	▪ Interview MFR (2 Pages) (Typed), 23 Jan 11
E49	[redacted] (SSG [redacted])
E49-1	▪ Canvass Interview Worksheet w/ Q&A, 11 Aug 10
E50	[redacted] (SPC [redacted])
E50-1	▪ DA Form 2823, Sworn Stmt (3 Pages) (Handwritten), 30 Jun 10

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

E50-2	INTENTIONALLY LEFT BLANK
E50-3	▪ AIR (Agent's Investigation Report) (3 Pages) (Typed), 6 Jan 11
E51	[redacted] (Mr. [redacted] (formerly SPC)
E51-1	▪ AIR (Agent's Investigation Report) (1 Page) (Typed), 4 Oct 10
E52	[redacted] (SPC [redacted])
E52-1	▪ DA Form 2823, Sworn Stmt (3 Pages) (Handwritten), 19 Jun 10
E53	[redacted] (CPT [redacted])
E53-1	▪ DA Form 2823, Sworn Stmt (2 Pages) (Handwritten), 24 Jun 10
E53-2	INTENTIONALLY LEFT BLANK
E53-3	▪ DA Form 2823, Sworn Stmt (3 Pages)(Typed), 18 Jan 11
E54	MAYFIELD (Mr. David Mayfield)
E54-1	▪ Interview MFR (1 Page) (Typed), 25 Jan 11
E55	INTENTIONALLY LEFT BLANK
E56	[redacted] (COL [redacted])
E56-1	▪ DA Form 2823, Sworn Stmt (5 Pages) (Typed), 20 Jan 11
E57	[redacted] (SGT [redacted])
E57-1	INTENTIONALLY LEFT BLANK
E57-2	▪ DA Form 2823, Sworn Stmt (2 Pages) (Typed), 23 Jun 10
E57-3	▪ Interview MFR (3 Pages) (Typed), 26 Jan 11
E58	[redacted] (SSG [redacted]
E58-1	▪ DA Form 2823, Sworn Stmt (3 Pages) (Handwritten), 21 Jul 10
E58-2	▪ Interview MFR (1 Page) (Typed), 24 Jan 11 (Noted – Date reads 2010 but was actually 2011)
E59	[redacted] (MAJ [redacted])
E59-1	▪ DA Form 2823, Sworn Stmt (2 Pages) (Handwritten), 10 Jun 10
E59-2	▪ MAJ [redacted] responses to Written Questions from MAJ [redacted] (Email Plus 2 Pages) (Typed), 21 Jul 10
E59-3	▪ Interview MFR (3 Pages) (Typed), 22 Jan 11
E60	[redacted] (Mr. [redacted])
E60-1	▪ 10 Jan 11 1:39 PM Email from Mr. [redacted]. to CW4 [redacted] Re: PFC Manning AIT SCIF Violation (2 Pages) (Typed)
E61	[redacted] (SGT [redacted]
E61-1	▪ Canvass Interview Worksheet w/ Q&As,11 Aug 10
E62	[redacted] (Mr. [redacted])
E62-1	▪ AIR (Agent's Investigation Report) (2 Pages) (Typed), 5 Oct 10
E63	[redacted] (SSgt [redacted])
E63-1	▪ AIR (Agent's Investigation Report) (2 Pages) (Typed), 25 Aug 10
E64	[redacted] (CPT [redacted])
E64-1	▪ DA Form 2823, Sworn Stmt (3 Pages) (Typed), 25 Aug 10
E65	[redacted] (SGT [redacted])
E65-1	▪ DA Form 2823, Sworn Stmt (3 Pages) (Typed), 21 Jan 11

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

E66	(b) (6), (b) (Mr. (b) (6), (b) (7)(C))
E66-1	▪ AIR (Agent's Investigation Report) (2 Pages) (Typed), 13 Oct 10
E67	(b) (6), (MSG (b) (6), (b) (7)(C))
E67-1	▪ DA Form 2823, Sworn Stmt (3 Pages) (Typed), 5 Jan 11
E68	(b) (6), (SSG (b) (6), (b))
E68-1	▪ Canvass Interview Worksheet w/ Q&As, 11 Aug 10
E69	(b) (6), (b) (LTC (b) (6), (b) (7))
E69-1	▪ Memo, SUBJECT: Question List for LTC (b) (6), (b) (7)(C) reference USF-I AR 15-6 Investigation (2 Pages) , 22 Jul 10
E70	(b) (6), (b) (7)(C) (SSgt (b) (6), (b) (7)(C))
E70-1	▪ AIR (Agent's Investigation Report) (2 Pages) (Typed), 20 Oct 10
E71	RAPP (CW2 (b) (6), (b) (7)(C))
E71-1	▪ AIR (Agent's Investigation Report) (3 Pages) (Typed), 27 Aug 10
E72	SAGEMAN (Dr. Marc Sageman)
E72-1	▪ Interview MFR (2 Pages) (Typed) 27 Jan 11
E73	(b) (6), (b) (SPC (b) (6), (b) (7)(C))
E73-1	▪ DA Form 2823, Sworn Stmt (4 Pages) (Typed), 28 May 10
E73-2	▪ DA Form 2823, Sworn Stmt (2 Pages) (Handwritten), 2 Jul 10
E73-3	INTENTIONALLY LEFT BLANK
E73-4	▪ Canvass Interview Worksheet w/ Q&As, 11 Aug 10
E74	(b) (6), (b) (SGT (b) (6), (b) (7)(C))
E74-1	▪ DA Form 2823, Sworn Stmt (2 Pages) (Handwritten), 15 Jun 10
E74-2	INTENTIONALLY LEFT BLANK
E74-3	INTENTIONALLY LEFT BLANK
E74-4	▪ DA Form 2823, Sworn Stmt (3 Pages) (Typed), 21 Jun 10
E74-5	▪ DA Form 2823, Sworn Stmt (2 Pages) (Handwritten), 11 Jul 10
E75	(b) (6), (SPC (b) (6), (b) (7)(C))
E75-1	▪ DA Form 2823, Sworn Stmt (2 Pages) (Typed), 8 May 10
E76	(b) (6), (b) (7) (Mr. (b) (6), (b) (7)(C))
E76-1	▪ AIR (Agent's Investigation Report) (2 Pages) (Typed), 7 Oct 10
E77	(b) (6), (b) (7) (SPC (b) (6), (b) (7)(C))
E77-1	▪ Canvass Interview Worksheet w/ Q&As, 11 Aug 10
E78	(b) (6), (b) (7) (SPC (b) (6), (b) (7)(C))
E78-1	▪ DA Form 2823, Sworn Stmt (2 Pages) (Handwritten), 8 May 10
E78-2	▪ DA Form 2823, Sworn Stmt (2 Pages) (Typed), 8 May 10
E78-3	▪ DA Form 2823, Sworn Stmt (5 Pages) (Handwritten), 18 Jun 10
E78-4	INTENTIONALLY LEFT BLANK
E78-5	▪ DA Form 2823, Sworn Stmt (4 Pages) (Typed), 19 Jan 11
E79	(b) (6), (b) (SPC (b) (6), (b) (7)(C))
E79-1	▪ DA Form 2823, Sworn Stmt (2 Pages) (Handwritten), 28 Jun 10
E80	(b) (6), (SSG (b) (6), (b) (7))

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

E80-1	▪ DA Form 2823, Sworn Stmt (2 Pages) (Typed), 8 May 10
E81	[redacted] (COL [redacted])
E81-1	▪ Memo, SUBJECT: Question List for COL [redacted] reference USF-I AR 15-6 Investigation (2 Pages) 21 Jul 10
E82	[redacted] (MSG [redacted])
E82-1	▪ DA Form 2823, Sworn Stmt (3 Pages) (Typed), 18 Jan 11
E82-2	▪ Interview MFR (1Page)(Typed), 05 Feb 11
E83	[redacted] (SPC [redacted])
E83-1	▪ Canvass Interview Worksheet w/ Q&As, 11 Aug 10
E84	[redacted] (SPC [redacted])
E84-1	▪ DA Form 2823, Sworn Stmt (3 Pages) (Handwritten), 28 May 10
E84-2	▪ DA Form 2823, Sworn Stmt (3 Pages) (Handwritten), 10 Jun 10
E84-3	▪ Interview MFR (2 Pages) (Typed), 25 Jan 11
E85	[redacted] (COL [redacted])
E85-1	▪ DA Form 2823, Sworn Stmt (5 Pages) (Typed), 5 Jan 11
E86	[redacted] (LTC [redacted])
E86-1	▪ Interview MFR (2 Pages) (Typed), 23 Jan 11
E87	[redacted] (GS13 [redacted])
E87-1	▪ DA Form 2823, Sworn Stmt (11 Pages) (Typed), 7 Jan 11
E88	[redacted] (PFC [redacted])
E88-1	▪ Canvass Interview Worksheet w/ Q&As, 11 Aug 10
E89	INTENTIONALLY LEFT BLANK
E90	[redacted] (CPT [redacted])
E90-1	▪ Interview MFR (2 Pages) (Typed) 24 Jan11
E91	[redacted] (MAJ [redacted])
E91-1	▪ DA Form 2823, Sworn Stmt (2 Pages) (Typed), 24 Jan 11
E92	[redacted] (LTC [redacted])
E92-1	▪ DA Form 2823, (15-6) Sworn Stmt (3 Pages) (Typed), 25 Jan 11
E93	[redacted] (SFC(R) [redacted])
E93-1	▪ CID Form 94, Stmt (3 Pages) (Typed) (Includes WO1 [redacted] SFC [redacted] SFC [redacted], MAJ [redacted] 1LT [redacted]) 10 Sep 10
E93-2	▪ CID Form 94, Stmt (1 Page) (Typed), 07 Feb 11
E93-3	▪ Interview MFR (15-6) (2 Pages) (Typed), 07 Feb 11
Tab F	**INTENTIONALLY LEFT BLANK**
Tab G	**Events Timeline**
G1	▪ Road to Wikileaks slides (3 Pages), 01 Feb 11
Tab H	**Organization Chart(s)**
H1	▪ Pre-Deployment Chain of Command and Technical Chain Re: PFC Manning
H2	▪ Deployment Chain of Command and Technical Chain Re: PFC Manning
H3	▪ 2/10 BCT S2 Section Organization Chart

H4	▪ Information Assurance/Information Security Hierarchy
Tab I	**Investigation Photos / Sketches**
I1	▪ 2/10 BCT SCIF Sketch (Room 14B, Bde HQ Bldg, FOB Hammer, Iraq)
Tab J	**Personnel Records – PFC Bradley E. Manning**
J1	▪ PFC Manning's personnel file
Tab K	**Counseling Records– PFC Bradley E. Manning**
K1	▪ PFC Manning's Counseling file
Tab L	**Medical Records – PFC Bradley E. Manning**
L1	▪ PFC Manning's medical records received from Fort Drum
Tab M	**Behavioral Health Records – PFC Bradley E. Manning**
M1	INTENTIONALLY LEFT BLANK
M1-1	▪ PFC Manning Command Referral (MEDCOM Form 4038), 25 Dec 09
M1-2	▪ 30JUN09 - PFC Manning SF 600 (Chronological Record of Medical Care)
M1-3	▪ 19AUG09 - PFC (b)(6) SF 600 (Chronological Record of Medical Care)
M1-4	▪ 15SEP09 - PFC Manning SF 600 (Chronological Record of Medical Care)
M1-5	▪ 23SEP09 - PFC Manning SF 600 (Chronological Record of Medical Care)
M1-6	▪ 29SEP09 - PFC Manning SF 600 (Chronological Record of Medical Care)
M1-7	INTENTIONALLY LEFT BLANK
M1-8	▪ 24DEC09 - PFC Manning SF 600 (Chronological Record of Medical Care)
M1-9	INTENTIONALLY LEFT BLANK
M1-10	▪ 30DEC09 - PFC Manning SF 600 (Chronological Record of Medical Care)
M1-11	▪ 06JAN10 - PFC Manning SF 600 (Chronological Record of Medical Care)
M1-12	▪ 16FEB10 - PFC Manning SF 600 (Chronological Record of Medical Care)
M1-13	▪ 02MAR10 - PFC Manning SF 600 (Chronological Record of Medical Care)
M1-14	▪ 16MAR10 - PFC Manning SF 600 (Chronological Record of Medical Care)
M1-15	▪ 23MAR10 - PFC Manning SF 600 (Chronological Record of Medical Care)
M1-16	▪ 30MAR10 - PFC Manning SF 600 (Chronological Record of Medical Care)
M1-17	▪ 06APR10 - PFC Manning SF 600 (Chronological Record of Medical Care)
M1-18	INTENTIONALLY LEFT BLANK
M1-19	INTENTIONALLY LEFT BLANK
M1-20	▪ 08MAY10 - PFC Manning SF 600 (Chronological Record of Medical Care)
M1-21	▪ 10MAY10 - PFC Manning SF 600 (Chronological Record of Medical Care)
M1-22	▪ 12MAY10 - PFC Manning SF 600 (Chronological Record of Medical Care)
M1-23	▪ 13MAY10 - PFC Manning SF 600 (Chronological Record of Medical Care)
M1-24	▪ 15MAY10 - PFC Manning SF 600 (Chronological Record of Medical Care)
M1-25	▪ 19MAY10 - PFC Manning SF 600 (Chronological Record of Medical Care)
M1-26	▪ 22MAY10 - PFC Manning SF 600 (Chronological Record of Medical Care)
M1-27	▪ 22MAY10 - Command referred Behavioral Health Report
M1-28	▪ 26MAY10 - PFC Manning SF 600 (Chronological Record of Medical Care)
M1-29	▪ 28MAY10 - PFC Manning SF 600 (Chronological Record of Medical Care)
M1-30	▪ 28MAY10 - Command referred Behavioral Health Report

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

Tab N	Personnel Records - Other
N1	SF 86 / Investigator Notes
N2	PFC Manning (JAMS), 28 Dec 10
N3	SF 86 Security Clearance Application, PFC Manning, 04 Nov 07
N4	PFC Manning OPM File
N5	Report of Unfavorable Information for Security Determination, DA Form 5248-R, Report of Unfavorable Information for Security Determination, 9 May 11 (Note – erroneously dated in original as 2011, however actual date is 2010)
N6	(ACICA) PFC Manning's Rights Warning Procedure/Waiver Certificate DA Form 3881, 08 May 10
Tab O	**Other**
O1	Oklahoma Police Record Investigation MFR, 14 Jan 11
O2	DD Form 2707, Confinement Order, 29 May 10
O3	PFC Manning (JAMS), 28 Dec 10
O4	Summary of Conversation and Email exchanges w/ Army G2 Personnel w/7 Attachments, 28 Jan 11
O4-1	PED Countermeasures Matrix
O5	PFC Manning Advance Fingerprint Report, 28 Oct 07
O6	OER, [redacted], OER Date: 28 Apr 09 – 17 Apr 2010
O7	VTC w/Fort Leonard Wood MSCoE Cadre and Department of the Army Investigate Team MFR, 28 January 2011
O8	Email from Ms [redacted] to LTC [redacted] 24 January 2011
O9	Information Assurance (IA) training & Real vs. Virtual Morals (Excerpts from email from [redacted] to COL [redacted] 19 Jan 11
O10	Wired.Com Excerpts
O11	USA Today, "Generation Y: They've arrived at work with a new attitude"
O12	Army Health Promotion, Risk Reduction, Suicide Prevention Report, 2010
O13	Email from PFC Bradley Manning to MSG [redacted], 24 Apr 10, 7:40 PM
O14	Email from COL [redacted] to LTC [redacted] regarding question on when PFC Manning accessed documents, Dated 21 Jan 11
O15	Email from COL [redacted] to COL [redacted] 27 Jan 11, Discussion regarding IA collective training from FORSCOM G6
O16	The 9/11 Commission Report
O17	Info Paper (MEDCOM), Access to PHI, 15 Sep 10, SUBJECT: HIPAA and Commander's Access to Soldier's Protected Health Information [PHI]
O18	Email from [redacted] to LTC [redacted] 01 Feb 11 Discussion of lies found by investigators during review of PFC Manning's SF86
O19	CPT [redacted] ORB (24 Jan 11)
O20	SSR 2LT [redacted], Training Completed, May 09

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

O21	The Telegraph (UK Article) Bradley Manning suspected source of Wikileaks documents scandal grew up in the Wales following family split
O22	2/10 BCT DIV TOC Layout
O23	DD Form 2807-1, Report of Medical History, Mar 07
O24	Mental Health Question, Standard Form (SF) 86, revised question 21 language, 18 Apr 08
O25	Email from Dr [redacted] to LTC [redacted], Addresses the possibility of PFC Manning's chain of command raising the issue of his security clearance being suspended, Dr [redacted] could not remember, 01 Feb 11
O26	Email from Ms [redacted] to LTC [redacted] addresses the policy of going on the internet and reviewing social media sites of individual – BLUF, we have not gone so far as to access individuals internet sites to farm information for security clearances, 01 Feb 11
O27	2/10 BCT 100-Day Review
O28	ATRRS Prerequisites for Course 243-35F10, Describes the prerequisites for a 35F before they go through their AIT
O29	Email from Ms [redacted] to LTC [redacted], discusses DCID 6/9 replaced by ICD 705
O30	Email from Manning to [redacted] (01 May 10)
O31	10th MTN SSR Training Slides, 111 Slides
O32	DoD SCI Security Officials Course Description
O33	(USD-C 380-5) CID Affidavit Supporting Reasonable Belief PFC Manning Released Classified Information, May 10
O34	Email from Mr [redacted] to LTC [redacted] regarding ICD 705 & ICS 705-1, 7 Feb 11
O35	Richard Mogull, "Understanding and Selecting a Data Loss Prevention Solution," Securosis.com white paper, 21 Oct 10
O36	15-6 Flag Paperwork, 7 Feb 11
O37	Millennials, Definition
O38	Wikileaks Afghanistan - leak inquiry centres on US intelligence analyst, The Telegraph Article (26 Jul 10)
O39	Defense Science Board 2006 Summer Study on "Information Management for Net-Centric Operatations" volume II, Apr 07
O40	Robert Sprague, "Rethinking Information Privacy in an Age of Online Transparency," 04 Feb 09
O41	Email from LCDR [redacted] to LTC [redacted], 2/10 TSCIF Certification Nov 09, 07 Feb 11
O42	Email from LCDR [redacted] to LTC [redacted] 2/10 TSCIF Decertification 26AUG10, 03 Feb 11
O43	Email from [redacted] to COL [redacted] discussion about MEDCOM Form 4038, 21 Jan 11
O44	DoD Task Force on Mental Health Report, "An Achievable Vision: Report of the Department of Defense Task Force on Mental Health Final Report," Jun 07

O45	Email from LTC (b) (6) to LTC (b) , reference IA personnel questions, 09 Feb 11
O46	(b) (6) Email to Park 11 Feb 11
Tab P	**Personnel Accountability Matrix**
P1	As of 05 Feb 11
Tab Q	**Policy/Regulatory/Statutory Excerpts**
Q1	DoDD 8500.01E, 24 Oct 02
Q2	CENTCOM Regulation 25-206
Q3	AR 25-2, 24 October 2007
Q4	MNF-I Directive 25-1
Q5	USF-I 25-1 v2, 15 March 2010
Q6	FM 6-02.71, Network Operations, 14 Jul 09
Q7	DoDI 8570.01-M, Information Assurance Workforce Improvement Program 19 Dec 05
Q8	USD-C IA Policy 6-1, Information Assurance/Computer Network Defense Policy and Procedures
Q9	NSTISSI No. 4012, Aug 97
Q10	NETCOM IA Training 05-PR-M-0002, 28 Feb 06, Information Assurance (IA) Training and Certification v4.0
Q11	AR 380-5, 29 Sep 00, Department of the Army Information Security Program
Q12	ALARACT, 245/2010, DTG: P 141042Z AUG 10
Q13	ALARACT, 246/2010, DTG: 170133Z AUG 10
Q14	ALARACT, 256-2010, DTG: P 211048Z AUG 10
Q15	ALARACT, 260-2010 DTG: P 260029Z AUG 10
Q16	AR 381-12, 4 Oct 10
Q17	ALARACT 322-2009
Q18	DoD Portable Electronic Device (PED) Policy, 25 Aug 06
Q19	DoDI 8570.01-M, 19 Dec 05
Q20	DoDI 8500.02, 6 Feb 01, Information Assurance Implementation
Q21	DoDD 5240.01, DoD Intelligence Activities
Q22	AR 381-12, 4 Oct 10, Threat Awareness and Reporting Program
Q23	AR 380-67, 9 Sep 88, The Department of the Army Personnel Security Program
Q24	DoD 5105.21-M-1, Aug 98, Sensitive Compartmented Information Administrative Security Manual
Q25	DCID 6-9, 18 November 2002, Director of Central Intelligence Directive No. 6/9 Physical Security Standards for Sensitive Compartmented Information Facilities
Q26	MEDCOM Form 4038, Undated, Report of Behavioral Health Evaluation
Q27	AR 635-200, 6 Jun 05, Active Duty Enlisted Administrative Separations

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

Q28	Director of Central Intelligence Directive No. 6/4, Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information, 02 July 1998
Q29	FORSCOM G6 Training Guidance, 17 Aug 09
Q30	DoD 8570.01-M, Information Assurance Workforce Improvement Program v2, 20 Apr 10
Q31	Personnel Security Investigations and Adjudications, 10 November 1998 These guidelines and investigative standards supersede that contained in Change 3 to DoD 5200.2-R, "DoD Personnel Security Program," dated February 23, 1996 and subsequent policy memoranda on the same subject
Q32	DA Pamphlet 611-21, Military Occupational Classification and Structure, 22 Jan 07
Q33	AR 25-1, Army Knowledge Management and Information Technology, 04 Dec 08
Q34	DA Form 5248-R, September 1983, Report of Unfavorable Information for Security Determination (DEROG)
Q35	MEDCOM Regulation 40-38, 1 Sep 01, Command Directed Mental Health Evaluations
Q36	DODD 6490.1 Excerpts
Q37	DODI 6490.4 Excerpts, Pages 1-13 and 1-1
Q38	DoD 6025.18-R, Jan 03, DoD HEALTH INFORMATION PRIVACY REGULATION
Q39	Directive-Type Memorandum (DTM) 09-006, 2 Jul 09 Revising Command Notification Requirements to Dispel Stigma in Providing Mental Health Care to Military Personnel
Q40	DODI 6400.6, 21 Aug 07 Domestic Abuse Involving DoD Military and Certain Affiliated Personnel
Q41	DODI 5210.42, 16 Oct 06, Nuclear Weapons Personnel Reliability Program (PRP)
Q42	Army G2 DAMI-CD Personnel Security Policy Summary, 28 Dec 10
Q43	ODCSINT Memo Re: DOD 5105.21-M-1, 4 Jun 01 Department of the Army Office of the Deputy Chief of Staff for Intelligence (ODCSINT) Memorandum, Subject: U.S. Army Implementation of Department of Defense 5105.21-M-1, Sensitive Compartmented Information
Q44	CENTCOM Regulation 380-12, 04 Aug 10 Sensitive Compartmented Information (SCI) Management
Q45	USF-I FRAGO 2242, 08 Nov 10 FRAGO 2242 USF-I Command Security SCIF/T-SCIF Inspection Program to USF-I OPORD 10.01
Q46	USF-I Command Security Response to Request for Information, 21 Jan 11
Q47	AR 600-37, Unfavorable Information

ATZL-CG
SUBJECT: AR 15-6 Report – Compromise of Classified Information to Wikileaks

Q48	Implementation of Adjudicative Guidelines for Determining Eligibility for Access to Sensitive Information, 30 Aug 06, Adjudication Standards
Q49	Intelligence Community Policy Guidance 704.2, 02 Oct 08, Personnel Security Adjudicative Guidelines for Determining Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information
Q50	(OBSOLETE) CENTCOM Regulation 380-12, Sensitive Compartmented Information (SCI) Management, 01 Mar 05
Q51	CENTCOM Regulation 380-3, Sensitive Compartmented Information (SCI) Access, 23 Oct 08
Q52	CENTCOM Regulation 380-1, Information Security Program Regulation, 01 Apr 07
Q53	T-SCIF Guidance for Army Units Deploying in support of Operation Enduring and Iraqi Freedom (OEF/OIF), 27 Feb 06
Q54	(OBSOLETE) AR 40-501, Standards of Medical Fitness, 29 May 07
Q55	AR 40-501, Standards of Medical Fitness, 23 Aug 10
Q56	AR 601-210, Active and Reserve Components Enlistment Program, 07 Jun 07
Q57	Intelligence Community Directive (ICD) 705, Sensitive Compartmented Information Facilities, 26 May 10
Q58	Intelligence Community Standard ICS 705-1, 17 Sep 10
Q59	Intelligence Community Standard (ICS) 705-2, Standards for the Accreditation and Reciprocal Use of Sensitive Compartmented Information Facilities, 17 Sep 10
Q60	ODNI (DRAFT) Technical Specifications for Construction and Management of SCIFs v10, XX Jan 11
Q61	DNI Policy Memorandum 2005-700-1, 01 Dec 05
Q62	Intelligence Community Directive (ICD) 704, Personnel Security Standards & Procedures Governing Eligibility for Access to Sensitive Compartmented Information & Other Controlled Access Program Information, 01 Oct 08
Q63	USF-I J2 SSO Operating Procedures
Q64	AR 40-66, Medical Record Administration and Healthcare Documentation, 4 Jan 10
Q65	DA Form 3822, Report of Mental Status Evaluation, Sep 09
Q66	Unified Command Plan, 17 Dec 08
Q67	AR 600-20, Army Command Policy, 27 Apr 10
Tab R	**Prior Investigations**
R1	USF-I AR 15-6 Investigation, 26 Jul 10
R2	USD-C AR 380-5 Investigation, 24 Jun 10