**DEPARTMENT OF THE ARMY**
OFFICE OF THE ASSISTANT SECRETARY
MANPOWER AND RESERVE AFFAIRS
111 ARMY PENTAGON
WASHINGTON, DC 20310-0111

November 26, 2008

The Honorable Scott J. Bloch
The Special Counsel
U.S. Office of Special Counsel
1730 M Street, N.W., Suite 300
Washington, D.C. 20036-4505

RE: Whistleblower Investigation – U.S. Army Training Support Center (ATSC), Fort Eustis, Virginia (OSC File DI-08-2159)

Dear Mr. Bloch:

In accordance with Title 5, United States Code (USC), Sections 1213 (c) and (d), the enclosed report is submitted in response to your referral of information requesting an investigation of allegations and a report of findings in the above-referenced case.

The Secretary of the Army (SA) has delegated to me his authority as agency head to review, sign, and submit to you the report required by Title 5, USC, Sections 1213(b), (c) and (d) [Tab A].

Note that this report and its exhibits contain the names and duty titles of employees, Soldiers, and contractor employees of the Army Training Support Center (ATSC) and Headquarters, U.S. Army Training and Doctrine Command (TRADOC), Fort Monroe, Virginia, as well as sexually explicit and inappropriate photographs and e-mails. Subsequent release of this information may result in violations of the Privacy Act,[1] and breaches of personal privacy interests. Accordingly, those releases required by Title 5, USC, Section 1213(e) excepted, the Department of the Army requests the opportunity to coordinate in advance on any release of this report outside the Office of Special Counsel.

## INFORMATION INITIATING THE INVESTIGATION

By letter dated July 23, 2008 [Tab B], the OSC referred to the SA its conclusion that information provided by a whistleblower, [redacted] disclosed that there was a substantial likelihood that Department of the Army employees and contractor personnel

[1] The Privacy Act of 1974 is codified at Title 5, USC, Section 552a.

at the ATSC, Fort Eustis, Virginia[2], may have engaged in activities that violated a law, rule, or regulation. Specifically, [redacted] alleged the following:

**OSC Allegation 1:** That based on her discovery of e-mails and photographs on the hard drive of the government computer of [redacted] (b)(6), Site Specialist, Video Teletraining Team (VTT), Individual Training Support Directorate (ITSD), ATSC—

**Allegation 1A:** [redacted] (b)(6) and [redacted] (b)(6), a contractor employee at the ATSC, had sent e-mails containing sexually explicit photographs from government e-mail accounts;

**Allegation 1B:** [redacted] (b)(6) an employee of Headquarters, TRADOC, Office of the Deputy Chief of Staff, G-3/5/7; [redacted] (b)(6) [redacted] (b)(6), former (now retired) Chief, VTT, ITSD, ATSC; contractor employee [redacted] (b)(6) [redacted] (b)(6) and contractor employee [redacted] (b)(6), sent e-mails from government e-mail accounts containing jokes, humor of a sexual nature, discussions of sexual encounters between employees, and other inappropriate material; and

**Allegation 1C:** [redacted] (b)(6) and [redacted] (b)(6) appeared in various states of undress in photographs appearing on a government computer hard drive.

all of which violated Army Regulation (AR) 25-1, *Army Knowledge Management and Information Technology*, paragraph 6-1f(1) **[Tab 3]**, and AR 25-2, *Information Assurance*, paragraph 4-5r(7) **[Tab 4]**.

**OSC Allegation 2:** That she had witnessed [redacted] (b)(6) and [redacted] (b)(6) [redacted] (b)(6), former (now retired) ATSC Training Support Acquisition Specialist, VTT, ITSD, ATSC, sharing government computer Common Access Cards (CACs) and passwords, in violation of AR 25-2, paragraphs 4-5a(8) and 4-5s(9).

## CONDUCT OF THE INVESTIGATION

By statute, an agency is afforded sixty (60) days to complete the report required by Title 5, USC, Section 1213. On July 28, 2008, the Office of Army General Counsel (OGC) forwarded the OSC request for investigation through the Office of the Staff Judge Advocate (OSJA), Headquarters, TRADOC, to the Office of the Staff Judge Advocate, Fort Eustis, for action **[Tab C]**. Although physically located at Fort Eustis, ATSC is an operating agency of Headquarters, TRADOC, Deputy Chief of Staff, G-3/5/7, located at Fort Monroe. Because an investigation into potential misconduct at ATSC and any subsequent corrective action would likely be taken at Headquarters, TRADOC, it was decided that OSJA, Headquarters, TRADOC, would assume responsibility for legal oversight of the investigation into the matters referred by OSC.

---

[2] Organization charts of Headquarters, TRADOC, the Deputy Chief of Staff, G-3/5/7, and ATSC are at Tabs 1 and 2, respectively.

On August 4, 2008, Major General (MG) Abraham Turner, the TRADOC Deputy Chief of Staff, G-3/5/7, appointed [redacted] (b)(6) as an Investigating Officer (IO) under the provisions of AR 15-6, *Procedures for Investigating Officers and Boards of Officers*,[3] to conduct an informal investigation into the allegations made by [redacted] **[Tab 5]**. Specifically, MG Turner appointed [redacted] (b)(6) to investigate the allegations that Federal employees [redacted] (b)(6) (now retired), and contractor employees [redacted] (b)(6) used government equipment and/or resources to transmit sexually explicit or inappropriate e-mail messages and photographs to other employees, or used government equipment and/or resources for any other purpose incompatible with public service, and to investigate whether any of the named employees improperly shared passwords and accessed other users' e-mail accounts, in violation of AR 25-1 and AR 25-2 **[Tab 5, p. 1, paras 3a-b]**. MG Turner further tasked [redacted] (b)(6) to ascertain whether there existed any systemic problem or mismanagement that had aided any misconduct determined to have occurred or allowed it to continue undetected until [redacted] submission of her allegations to OSC **[Tab 5, p. 1, para 3c]**. Finally, [redacted] (b)(6) was directed to investigate and report on any additional violations of law, rule, or regulation he discovered by any persons during the course of his investigation **[Tab 5, p.1, para 3d]**.

During his investigation, as memorialized in the Report of Investigation (ROI) **[Tab 6]**, [redacted] (b)(6) gathered documentary evidence in the form of e-mails and photographic attachments sent to and among Federal and contractor employees, primarily at ATSC, Fort Eustis. He also interviewed seventeen (17) persons associated with the allegations, including key witnesses [redacted] (b)(6) [redacted] (b)(6) and Ms. Ahrens **[Tab 6, Exhibit V, Statement of** [redacted] (b)(6)**; Exhibit S, Statement of** [redacted] (b)(6)**; Exhibit R, Statement of** [redacted] (b)(6)**; Exhibit Q, Statement of** [redacted] (b)(6)**; Exhibit T, Statement of** [redacted] (b)(6)**; Exhibit K, Statement of** [redacted] (b)(6)**; and Exhibit B, Statement of** [redacted]**]**. In the context of these interviews the IO obtained thirteen (13) sworn statements, four (4) "official" memoranda of record, one certified e-mail statement, and records of his conversations with [redacted] (b)(6)

On August 14, 2008, the AR 15-6 IO completed his findings and recommendations, and submitted his ROI to the Headquarters, TRADOC OSJA for legal review, as his legal advisor had instructed **[Tab 6, pp. 6-8, paras III-IV]**. As to the specific allegations referred by OSC, the IO found that--

(1) [redacted] (b)(6) improperly used government equipment to transmit sexually explicit and other inappropriate material in violation of AR 25-1, paragraph 6-1f(1)[4] and AR 25-2, paragraph 4-5r(7)[5];

---

[3] AR 15-6 promulgates guidelines for Army administrative investigations. Army commands and organizations appoint investigating officers (IOs) under provisions of AR 15-6 to investigate all manner of allegations and concerns.

[4] This provision prohibits "Use of communications systems that would adversely reflect on the Department of Defense (DoD) or the Army (such as uses involving sexually explicit e-mail or access to sexually explicit Web sites, pornographic images, or virtual computer-generated or otherwise pornographic images)."

(2) He could not determine whether (b)(6) (a contractor employee) used either a government computer or his personal computer to transmit sexually explicit and other inappropriate material because (b)(6) used both his personally owned and government-issued computer in the context of his work at the ATSC.[6] The IO did determine, however, that (b)(6) transmitted multiple sexually explicit and inappropriate e-mails from his Army Knowledge Online (AKO) e-mail account, (b)(6) **[Tab 6, Exhibit F, pp. 48-92]**;

(3) Although the evidence indicates that (b)(6) received from (b)(6) sexual explicit e-mail and e-mail containing other inappropriate material **[Tab 6, Exhibit F, pp. 48-92]**, there is no evidence that they transmitted these e-mails to others outside their group **[Tab 6, Exhibit L, Statement of** (b)(6) **Exhibit Q, Statement of** (b)(6) **Exhibit R, Statement of** (b)(6) (b)(6) **Exhibit S, notes from meeting with** (b)(6)**]**;

(4) No evidence indicates that (b)(6) is or was a member of the armed forces, a Federal employee, or a Federal contractor employee **[Tab 6, Exhibit U, Statement of** (b)(6) (b)(6)**]**;

(5) (b)(6) improperly shared and (b)(6) (b)(6) improperly used government CACs and computer passwords in violation of AR 25-2, paragraph 4-5a(8)[7] **[Tab 6, Exhibit B, Statement of** [redacted] **Exhibit C, Statement of** (b)(6) **Exhibit D, Statement of** (b)(6)**; and Exhibit V, Statement of** (b)(6)**]**;

(6) Although (b)(6) acquiesced or allowed (b)(6) (b)(6) to use their respective CACs and computer passwords to access their government computers, their actions were impermissible under provisions of AR 25-2, paragraph 4-5s(9)[8] **Tab 6, Exhibit B, Statement of Ms.** [redacted] **Exhibit C, Statement of** (b)(6)**; Exhibit D, Statement of** (b)(6)**; and Exhibit V, Statement of** (b)(6)**]**;

(7) (b)(6) the Director, ATSC, failed to provide effective leadership in addressing these issues when they were brought to his attention in that he focused on the conduct of [redacted] the individual making the report, rather than on the underlying violations, thereby creating a perception that management tolerated the inappropriate

---

[5] This provision prohibits "any personal use of Government resources involving: pornography or obscene material (adult or child): . . ."

[6] (b)(6) stated he had sent (b)(6) "adult-content" images, but denied sending anything pornographic and, to the best of his memory, has never sent her "adult-content" images on Army Knowledge on Line (AKO) or government systems **[Tab 6, Exhibit T, Notes from a meeting between** (b)(6) (b)(6) **IO, and** (b)(6)**, paras 4 and 6]**.

[7] This provision prohibits "[s]haring personal accounts and authenticators (passwords or PINs) . . . with any unauthorized individual."

[8] This provision prohibits, with exceptions not applicable here, Army personnel and contractors "from browsing or accessing other user's e-mail accounts."

conduct and would not effectively deal with complaints concerning that conduct [Tab 6, Exhibit B, Statement of [redacted] Exhibit I, Statement of [redacted] (b)(6) Exhibit J, Statement of [redacted] (b)(6) [redacted], and Exhibit K, Memorandum of [redacted] (b)(6) [redacted] (b)(6) [redacted] interview].

Accordingly, the AR 15-6 IO recommended that:

(1) [redacted] (b)(6) [redacted] supervisors take appropriate remedial and disciplinary action against her for violations of AR 25-1 and AR 25-2;

(2) [redacted] (b)(6) [redacted] supervisors take appropriate remedial and disciplinary action to address his failure to exercise appropriate leadership and use sound judgment in his attempts to resolve the issues identified in this investigation when they were made known to him in May 2008;

(3) ATSC leaders receive appropriate professional training designed to enhance their ability to lead their organization effectively and to respond appropriately to Equal Employment Opportunity issues; and

(4) Headquarters, TRADOC, Deputy Chief of Staff, G-3/5/7 leaders review the ATSC supervisory structure and rating schemes to ensure all employees and managers are supervised and rated appropriately and fairly.

On August 19, 2008, [redacted] (b)(6) [redacted] Chief, Military Law Division, OSJA, TRADOC, completed a legal review of the investigation and determined that the proceedings complied with the legal requirements, there were no appointing or substantial errors, the evidence was sufficient to support the IO's findings, and the recommendations were consistent with the findings [Tab 7 ]. On August 21, 2008, [redacted] (b)(6) [redacted] Acting SJA, TRADOC, endorsed [redacted] (b)(6) [redacted] legal review and determined that the investigation was legally sufficient. He recommended that the appointing authority, MG Turner, approve the IO's findings and recommendations [Tab 8]. MG Turner approved the findings and recommendations on August 26, 2008 [Tab 9].

In order to ensure completion of the subject investigation and to prepare and staff the Army's final report to the OSC, the Army OGC requested one extension of time from the OSC. The request for extension was submitted on September 22, 2008 and was granted by the OSC on September 23, 2008, thus extending the period allowed for the Army to submit its response until November 24, 2008. [Tab D].

## SUMMARY OF EVIDENCE OBTAINED FROM THE INVESTIGATION

The evidence regarding the OSC-referred allegations that government and contractor employees improperly used Army communications systems for purposes involving transmission of sexually explicit and other inappropriate material, and that government

employees improperly shared government CACs and passwords to access other users' government e-mail accounts is summarized below.

**OSC Allegation 1:** Federal employees and contractors have been sending e-mails containing sexually explicit and inappropriate photographs and jokes, humor of a sexual nature, discussions of an obscene nature, and other inappropriate material from government e-mail accounts during duty hours, in violation of AR 25-1 and AR 25-2.

**Allegation 1A:** Federal employee [redacted] (b)(6) and contractor [redacted] (b)(6) have sent e-mails from government e-mail accounts containing explicit pornographic images;

**Allegation 1B:** [redacted] (b)(6) Federal employees [redacted] (b)(6) [redacted] (b)(6) (retired), and contractor employees [redacted] (b)(6) [redacted] (b)(6) have sent e-mails from government e-mail accounts containing jokes and humor of a sexual nature, discussions of sexual encounters between employees, and other inappropriate material.

**Allegation 1C:** [redacted] (b)(6) appeared in various states of undress in photographs on the hard drive.

**Relevant Authorities:**

(1) AR 25-1, *Army Knowledge Management and Information Technology*, July 25, 2005, establishes Army policies and assigns responsibilities for the management of information resources and information technology [Tab 3]. AR 25-1, Chapter 6, concerns command, control, and computer technology support and services. Paragraph 6-1f(1) states the following prohibition:

> Use of communications systems that would adversely reflect on DOD or the Army (such as uses involving sexually explicit e-mail or access to sexually explicit Web sites, pornographic images, or virtual computer-generated or otherwise pornographic images); . . . and other uses that are incompatible with public service.

(2) AR 25-2, *Information Assurance*, October 24, 2007, establishes information assurance policy, roles, and responsibilities [Tab 4]. AR 25-2, Chapter 4, addresses information assurance policy. Paragraph 4-5r(7) indicates:

> Certain activities are never authorized on Army networks. AUPs[9] will include the following minimums as prohibited. These activities include any personal use of Government resources involving: pornography or obscene material (adult or child;

**Discussion:**

[9] "AUP" denotes "Authorized Use Policy." *See* Tab 4, AR 25-2, Glossary.

The AR 15-6 IO began his investigation on August 4, 2008, and ascertained the following facts.

On February 5, 2008, (b)(6) (Federal employee, GS-09), at ATSC, Fort Eustis, was reassigned from the VTT, where she served under the second-line supervision of to the Training Support Services Division (TSSD), under the second-line supervision of (b)(6) (Federal employee, YA-03) [Tab 6, Exhibit B, Statement of p. 2, "SPECIAL DETAIL"; Tab G. Statement of (b)(6) (b)(6) para 2c]. On February 8, 2008, Ms. Ahrens provided her supervisor, (b)(6) (b)(6) Director, ITSD, ATSC (b)(6) retired from Federal service in April 2008) with a list of actions/issues that (b)(6) would need either to complete or to transfer to another employee in the VTT in order to close out (b)(6) service in s division. One required "close-out" item was the transfer of certain work-related program files from (b)(6) government computer (as well as the transfer of work-related paper files on the same subjects) to another VTT employee who would continue to work with the files after (b)(6) departure. Ms. Ahrens did not want (b)(6) government computer to be replaced because she was concerned that information important to the operation of the VTT and stored on that computer would be lost. After (b)(6) retired from federal service in April 2008, (b)(6) assumed duties as the Acting Director, ITSD in addition to continuing in his role as supervisor of the TSSD. then sought (b)(6) assistance in ensuring that (b)(6) completed the transfer of the VTT workplace files from her computer.

On or around February 12, 2008, (b)(6) the Systems Administrator and a contractor employee at ATSC, "re-ghosted"[10] an existing TSSD computer for (b)(6) (b)(6) copying all of the data and files from her old VTT computer to the new TSSD computer [Tab 6, Exhibit A, Statement of (b)(6) p. 1].

On April 30, 2008, (b)(6) was in the process of replacing old government computers with newer models and conducted a life cycle replacement of the government computer formerly used by (b)(6) during her service in VTT. Pursuant to ATSC procedure, he asked (b)(6) former second-level supervisor, if she needed any of the data remaining on (b)(6) old computer. As previously stated, wanted to retain historical knowledge of certain of the workplace programs on which (b)(6) had worked and thus requested that (b)(6) transfer the data from (b)(6) VTT computer to the ATSC shared portal. When (b)(6) had difficulty transferring the data from (b)(6) as had requested, Ms. indicated that she could attempt to retrieve the information herself but wanted to continue to seek (b)(6) cooperation in transferring the files. (b)(6) removed the hard drive from (b)(6) old computer and gave it to Ms. Ahrens to hold [Tab 6, Exhibit A, Statement of (b)(6) p. 1; Exhibit B, Statement of Ms. Sheila Ahrens, p. 2, "DISCOVERY"].

[10] "Re-ghosting", or "re-imaging", is the process of copying or purging unwanted files and data from a computer while leaving the remaining files intact.

As of May 13, 2008, [redacted] had not received from [redacted] (b)(6) the VTT workplace historical files she had requested, nor had [redacted] (b)(6) transferred the files to another employee in the VTT [Tab 6, Exhibit B, Statement of [redacted] p. 2, "DISCOVERY"].

Accordingly, on May 14, 2008, [redacted] took her government laptop computer and the hard drive from [redacted] (b)(6) former computer to her ([redacted] home. [redacted] intended to attempt to transfer [redacted] (b)(6) workplace historical files from the old hard drive to [redacted] government laptop for subsequent transfer to VTT office files. Further, [redacted] intended to retrieve data from the old hard drive pertaining to a special project to which she had been assigned—to assist in resolving certain property inventory issues that were the subject of an ongoing AR 15-6 investigation.[11] [Tab 6, Exhibit B, Statement of [redacted] p. 1, "SPECIAL DETAIL"; p. 2, "DISCOVERY", para 3; Exhibit N, Statement of [redacted] (b)(6) p. 1]. [redacted] (b)(6) [redacted] (b)(6) and a Federal employee, assisted her in connecting the hard drive to her laptop. [redacted] was able to read the hard drive and began searching it and downloading files she believed to be relevant to her work. In the process, [redacted] discovered sexually explicit and other inappropriate images and PowerPoint presentations within e-mail folders. It appeared that [redacted] (b)(6) had e-mailed these images to Soldiers, other Federal employees, and Federal contractor employees. [redacted] printed a sample of the offensive material she found on the hard drive, as "evidence of numerous infractions" committed by government and contractor employees and gave them to [redacted] (b)(6) ATSC Deputy Director (Federal employee, YC-03), on or about May 19, 2008. [redacted] asked [redacted] (b)(6) if the material would be reviewed by leadership with follow-up discussion to determine how to best proceed [Tab 6, Exhibit B, Statement of [redacted] p. 2, "DISCOVERY", para 4; Exhibit F, e-mail messages and photo images, pp. 1-107; Exhibit G, Memorandum Statement of [redacted] (b)(6) pp. 2-3, para 3c].

The materials discovered by [redacted] and provided to [redacted] (b)(6) contained inappropriate images of [redacted] (b)(6) (Federal employee, GS-13) in undergarments; sexually explicit images and materials attached to e-mails sent to [redacted] (b)(6) (contractor employee), dated September 12, 2006; sexually explicit material sent to [redacted] (b)(6) (now retired Federal employee)[12], dated June 5, 2006; sexually explicit material sent to Army Sergeant [redacted] (b)(6), dated June 2, 2006; an inappropriate image attached to e-mail sent to [redacted] (b)(6) dated March 9, 2006; sexually explicit material in a PowerPoint presentation attached to e-mail sent to [redacted] (b)(6) dated December 9, 2005; and inappropriate images attached to e-mail sent to numerous recipients, dated November 2, 2005. There was also sexually explicit material attached to incoming e-mails received by [redacted] (b)(6) from [redacted] (b)(6) dated December 9, 2005 and June 2 and 5, 2006 [Tab 6, Exhibit F, Printed e-mail messages and images, pp. 1-107].

---

[11] Note that this AR 15-6 is wholly separate and apart from the AR 15-6 investigation appointed in response to the Army's receipt of the OSC-referred allegations.

[12] [redacted] (b)(6) retired from federal service before the OSC referred the subject allegations to the Secretary of the Army on July 23, 2008.

(b)(6) delivered the images and PowerPoint presentations provided by to the Director, ATSC, (b)(6) (Federal employee, YC-03) on or about May 20, 2008. (b)(6) in turn, consulted the Army Criminal Investigation Division (CID)[13] at Fort Eustis, as well as with the ATSC Support Directorate for guidance [Tab 6, Exhibit K, Memorandum Statement of (b)(6), p. 1, para 2; Exhibit L, Statement of (b)(6)]. On the advice of local government attorneys, (b)(6) instructed the Support Directorate to seize (b)(6) removed hard drive, government computer, (b)(6) old government computer, and (b)(6) (b)(6) new government computer on May 22, 2008 [Tab 6, Exhibit B, Statement of , p. 3, "DISCOVERY", para 7; Exhibit G, Memorandum Statement of (b)(6) p. 3, para 3d; Exhibit K, Memorandum Statement of (b)(6) (b)(6) p. 1, para 3; Exhibit L, Statement of (b)(6) p. 1]. CID personnel informed (b)(6) that s actions culminating in her discovery of the offensive materials on (b)(6) old hard drive may have been improper and may warrant a "hand slap" [Tab 6, Exhibit K, Memorandum Statement of (b)(6) (b)(6), p. 1, para 3a]. However, CID advised (b)(6) that it would become involved in investigating the matter only if child pornography was discovered on the hard drive at issue or on any of the government computers.[14] There was not then, and is not now any indication that any of the images or activities associated with this investigation involve child pornography [Tab 6, Exhibit K, Memorandum Statement of (b)(6), p. 1, para 3b]. CID also advised that there was "a possibility that government employees may have arranged a tryst at government expense" but that if any such Temporary Duty (TDY) had been for a valid mission, CID would not generally get involved in the investigation [Tab 6, Exhibit K, Memorandum Statement of (b)(6), p. 1, para 3c]. (b)(6) informed his superior of the foregoing on or about May 23, 2008 [Tab 6, Exhibit K, Memorandum Statement of (b)(6), p. 2, para 4].

On May 27, 2008, (b)(6) hosted a meeting with (b)(6) (b)(6) and with the understanding among the latter three that they would discuss the "way ahead" regarding discovery [Tab 6, Exhibit B, Statement of Ms. Sheila Ahrens, p. 3, "DISCOVERY", para 4; Exhibit G, Memorandum Statement of (b)(6) p. 3, para 3e; Exhibit I, Statement of (b)(6) p. 1, paras 1, 2; Exhibit J, E-mail narrative of IO, adopted by (b)(6) p. 1, paras 4, 5]. However, (b)(6) focused the discussion primarily on a single e-mail string between (b)(6) and himself[15] that in his view inaccurately suggested an inappropriate relationship between (b)(6) [Tab 6, Exhibit I, Statement of (b)(6) p. 1, paras 3 and 5; Exhibit J, E-mail narrative of IO, adopted by (b)(6) p. 1, para 4] and on the methods had

[13] The Army Criminal Investigation Command is more commonly known as the Criminal Investigation Division (CID). Many of the witnesses refer to the CIC as "CID."

[14] CID policy with regard to the investigation of child and adult pornography is set forth contained in CID Regulation 195-1, *Criminal Investigation Operational Procedures*, Chapter 13, Computer Crime and Electronic Evidence, para 13-8 [Tab L].

[15] The e-mail exchange between (b)(6) on December 13, 2004, concerned an invitation for (b)(6) to attend a holiday potluck meal for ATSC personnel. However, (b)(6) reply to (b)(6) could be viewed as inappropriately familiar. [Tab 6, Exhibit F, p. 46].

employed in discovering the materials at issue. (b)(6) went so far as to read to Ms. Ahrens the Table of Penalties for employee misconduct[16] [Tab 6, Exhibit B, Statement of Sheila Ahrens, p. 3, 4, "DISCOVERY", paras 4-6; Exhibit B-J; Exhibit I, Statement of (b)(6) p. 1, paras 4-6; Exhibit J, E-mail narrative adopted by (b)(6), paras 5, 6]. (b)(6) did not address the organization's response to (b)(6) possible misuse of government computers in transmitting inappropriate and sexually explicit e-mail. (b)(6) believes (b)(6) not only failed to address the issue, but failed to understand command responsibilities regarding [redacted]s discovery [Tab 6, Exhibit J, E-mail narrative adopted by (b)(6), para 8].

On June 3, 2008, (b)(6) received two directives from his supervisor, Mr. Robert Seger, a member of the Senior Executive Service (SES) assigned as the Assistant Deputy Chief of Staff, G-3/5/7, Headquarters, TRADOC. First, pursue appropriate administrative action against ATSC employees who had maintained pornography on their government computers; second, determine whether there was any indication (b)(6) (b)(6) had used government travel to facilitate or further any sexual liaisons with other employees or government contractors.

Pursuant to a request from (b)(6), and at the direction of their supervisor, (b)(6) (b)(6), Chief, Support Division , ATSC, (b)(6) (Federal employee, GS-12) and (b)(6) (Federal employee, GS-11) used computer scans to review the content of (b)(6) new computer in TSSD in early May 2008 [Tab 6, Exhibit K, Memorandum Statement of (b)(6) p. 1, para 3a; Exhibit G, Memorandum Statement of (b)(6), Enclosures 3, 4; Exhibit L, Statement of (b)(6), p. 1;]. They did find the same inappropriate images and e-mails on (b)(6) (b)(6) computer as [redacted] had previously found, but did not discover any additional sexually explicit material on the computer. On July 3, 2008, (b)(6) and (b)(6) provided copies of the materials gleaned from the scan of (b)(6) computer to (b)(6) [Tab 6, Exhibit G, Memorandum Statement of (b)(6) (b)(6) Enclosure 3; Exhibit K, Memorandum Statement of (b)(6), p. 2, para 4a]. Computer scans revealed no sexually explicit material or inappropriate images on (b)(6) old or new computers, or on [redacted] computer [Tab 6, Exhibit L, Statement of (b)(6) p. 1; Exhibit G, Memorandum Statement of (b)(6) (b)(6) Enclosures 3, 4].

(b)(6) tasked his deputy, (b)(6) to undertake the first tasker set forth above.[17] Concerning the second tasker, (b)(6) personally reviewed (b)(6)

---

[16] AR 690-700, *Personnel Relations and Services (General)*, Chapter 751, Table 1-1, Table of Penalties for Various Offenses.

[17] (b)(6) informal investigation into this matter is reflected in his Memorandum for Record of July 22, 2008 [Tab 6, Exhibit G, Memorandum Statement of (b)(6)] and in his memorandum of August 7, 2008 to the IO [Tab 6, Exhibit H, Memorandum Statement of (b)(6)]. There is no further record of (b)(6) investigation. (b)(6) concluded his investigation by stating that since (b)(6) (b)(6) was not responsive to Ms. Ahrens's request for her historical files, Ms. Ahrens was "fully justified" in her actions to extract these historical files from (b)(6) government computer. (b)(6) (b)(6) points out that (b)(6), the Fort Eustis Director of Information Management, had determined that Ms. Ahrens had not violated AR 25-2, which prohibits "fishing expeditions" by Army

TDY records from December 2002 through February 2007. [redacted] (b)(6), Acting Director, Distance Learning Directorate (dLD), Office of the Deputy Chief of Staff, G-3/5/7, Headquarters, TRADOC, reviewed [redacted] (b)(6) TDY records for the same period. A comparison of the two record sets found no TDY correlation. Accordingly, [redacted] (b)(6) determined that the two employees had not improperly used government funds or travel for personal reasons [Tab 6, Exhibit. K, Statement of [redacted] (b)(6) p.2, para 4].

Because [redacted] (b)(6) never advised [redacted]s that he had directed [redacted] (b)(6) to investigate the inappropriate materials found on [redacted] (b)(6) hard drive, [redacted] believing that her concerns were not being addressed, solicited her husband's help in using the "open door" policy[18] to bring these matters to the attention of [redacted] (b)(6) SES supervisor, Mr. Seger. [redacted] (b)(6) presented [redacted] (b)(6) concerns to [redacted] (b)(6) (Federal employee, YA-03), Mr. Seger's deputy (note that [redacted] (b)(6) did not provide [redacted] (b)(6) with any of the inappropriate materials that had been discovered). [redacted] (b)(6) [redacted] (b)(6) in turn, consulted with [redacted] (b)(6) TRADOC OSJA Labor Counselor, and then informed Mr. Seger of the general nature of the situation. [redacted] (b)(6) did not discuss specific allegations with Mr. Seger because he did not wish to compromise Mr. Seger's objectivity in the matter, given that Mr. Seger could be called upon subsequently to review evidence and make decisions. Further, [redacted] (b)(6) offered [redacted] the opportunity to meet personally with him (not with Mr. Seger), to discuss with him, first-hand, her concerns and knowledge of the situation and to provide him with copies of the inappropriate materials. [redacted]s declined to meet with [redacted] (b)(6) also informed [redacted] (b)(6) that he could use the "open door" policy to meet with Mr. Seger, but that he ([redacted] (b)(6)) advised against it because such action could compromise Mr. Seger's future ability to make fair and objective decisions in the matter [Tab 6, Exhibit B, Statement of Ms. Sheila Ahrens, p. 4, "DISCOVERY", para 2; Exhibit

---

personnel by accessing and browsing through the government e-mail accounts of others [Tab 6, Exhibit G, Memorandum Statement of [redacted] (b)(6), p. 3, paras 4 and 5]. It is important to understand, however, that the statements of [redacted] (b)(6) [redacted] and [redacted] (b)(6) also reference an AR 15-6 investigation in which the appointed IO was [redacted] (b)(6) [redacted] had been detailed specially to assist [redacted] (b)(6) with his effort [Tab 6, Exhibit B, Statement of [redacted] pp. 1-2, "SPECIAL DETAIL", "DISCOVERY", para 3; Exhibit D, Statement of [redacted] (b)(6) p. 2, para 6; Exhibit G, Memorandum Statement of [redacted] (b)(6) pp. 1,2, para 2 ]. That investigation concerned property accountability issues for which an AR 15-6 investigation was appropriate under AR 735-5, *Policies and Procedures for Property Accountability*, paragraph 13-25, and it is not relevant to the matters referred to the Army by OSC or to the issues central to the instant report. Further, [redacted] (b)(6) [redacted] and [redacted] (b)(6) [redacted] (b)(6) reference yet another informal investigation by [redacted] (b)(6) Director, ITSD, ATSC, in January 2008, into alleged inappropriate office behavior. [redacted] (b)(6) retired in April 2008. Her investigation was self-initiated and, although she did interview some witnesses and take statements, no findings or recommendations were ever reduced to writing; however, [redacted] (b)(6) investigation did prompt [redacted] (b)(6) to direct a sensing session for the VTT employees in early 2008, and was the basis for [redacted] (b)(6) reassignment from VTT to TSSD [Tab 6, Exhibit B, Statement of [redacted], p. 2, "SPECIAL DETAIL", para 1; Exhibit D, Statement of [redacted] (b)(6) p. 3, paras 1, 3; Exhibit G, Memorandum Statement of [redacted] (b)(6), p. 2, 5, paras 2b, 5 ].

[18] It is common for Army officers and civilian senior leaders to maintain an "open door policy." Such a policy usually provides that any person may schedule a meeting with the officer or leader at any time to discuss matters of concern. Such policies are intended to eliminate bureaucratic barriers between employees and their commanders, supervisors, and leaders.

M, Statement of (b)(6), p. 1; Exhibit N, Statement of (b)(6) pp. 1, 2].

The IO appointed to investigate the OSC-referred allegations reviewed (b)(6) (b)(6) e-mail folders (current as of August 2008) in her new computer (that now contained both that data and files that (b)(6) had copied from her old computer to her new computer as well as additional items she had added to her new computer since being reassigned to TSSD. The IO discovered additional sexually explicit inappropriate images and movies stored on (b)(6) computer, primarily in her "sent" and "deleted" folders [Tab 6a, p. 6, para II(s)]. The images included personal sexually explicit images.[19] The IO's discovery included all of the images and PowerPoint presentations originally discovered by in her review of (b)(6) hard drive. The IO's review determined that (b)(6) files were dominated by legitimate government work, but did contain sexually explicit images scattered throughout sporadically. The images from (b)(6) e-mail files were consolidated on five compact discs.[20] .

(b)(6) concluded, and the IO appointed to investigate the OSC-referred allegations found specifically that , acting in her supervisory role, was authorized to examine the hard drive from (b)(6) old government computer for relevant office historical files and to assist an AR 15-6 IO[21] in a property accountability investigation [Tab 6, Exhibit G, Memorandum Statement of (b)(6) encl 4]. Therefore, actions regarding (b)(6) hard drive were not inappropriate and comported with AR 25-2, paragraph 4-5a(7).[22]

---

[19] (b)(6) discovery is admittedly inconsistent with (b)(6) review in May 2008 (*See supra* p. 10) in that (b)(6) found more information and images than did (b)(6) and (b)(6) The probable explanation is that (b)(6) "did not find everything I found because the additional material was added after they reviewed the e-mail folders in May, or because my advanced academic training enabled me to discover that material." [Tab E, Statement of (b)(6) (b)(6)]. (b)(6) possesses a Ph.D. in Systems and Information Engineering, and is a data mining expert; his expertise in these matters likely facilitated the discovery of this additional material [Tab E, Statement of (b)(6)].

[20] These materials found by (b)(6) and referenced in his report at Tab 6, Exhibit X, have not been included with this report as they contain material in addition to what was included in the OSC referral. These materials comprise additional sexually explicit and other inappropriate matter. These materials are maintained in Army files and are available for review, as appropriate.

[21] Recall that was specially detailed to assist another AR 15-6 IO, (b)(6) in an investigation of property accountability issues unrelated to the allegations referred to the Army by OSC. *See supra* note 14.

[22] We agree with this conclusion. In the case of *O'Connor v. Ortega*, (480 US 709, 725 (1987)), the Supreme Court expressed the view that "to ensure the efficient and proper operation of government agencies, public employers must be given wide latitude to enter employee offices for work-related, non-investigatory reasons," and that "work-related searches are merely incident to the primary business of the agency." The Court thus held that searches for both non-investigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of "reasonableness under the circumstances." In this case, s search of the computer hard drive for work-related documents to retrieve historical workplace files, as well as to assist in the investigation being conducted by (b)(6) was reasonable. As to s search for workplace historical files, the search was non-investigatory and reasonably limited to the place where the documents were stored, the hard drive of (b)(6) (b)(6) computer. As to search for the information relating to (b)(6) AR 15-6

(b)(6), who worked in the Office of the G-3/5/7, Headquarters, TRADOC , and was thus the only Federal employee referenced in this investigation not performing duties at ATSC, acknowledged having received "adult explicit material" via email on his government account from (b)(6) in the past, but stated that he had deleted and had not forwarded the inappropriate e-mails[Tab 6, Exhibit R, Statement of (b)(6) p. 1]. However, the evidence indicates that (b)(6) authored one lengthy e-mail message to (b)(6) which was discovered by [redacted] The message was dated November 4, 2003, at 1:19 o'clock P.M., had been sent to (b)(6) from (b)(6) Army e-mail address, and was clearly sexually suggestive in nature [Tab 6, Exhibit F, Printed e-mail messages and images, p. 10].

(b)(6) now retired from Federal service, refused to provide a statement to the IO, but did emphasize that he did not understand the allegations regarding (b)(6) He referred to her as a "churchgoing woman" and a "loving grandmother" [Tab 6, Exhibit S, Notes from meeting between (b)(6) 1-4]. Regardless, the record contains a significant number of suggestive e-mail message exchanges between (b)(6) during 2002, 2005, and 2006. Throughout this period of time, (b)(6) was (b)(6) first-line supervisor; almost all of the e-mails at issue were exchanged during regular duty hours [Tab 6, Exhibit F, Printed e-mail messages and images, pp. 11-22].

(b)(6) (contractor employee), did not recall receiving sexually explicit e-mail from (b)(6) He asserted that he deleted and did not forward any inappropriate e-mail he had received [Tab 6, Exhibit Q, Statement of (b)(6) p. 1]. Regardless, the record contains a number of e-mail messages exchanged between (b)(6) (b)(6) and (b)(6) the majority of which were exchanged during regular duty hours and were extremely sexually suggestive in nature [Tab 6, Exhibit F, Printed e-mail messages and images, pp. 95-99, 101-107 ].

(b)(6) is a contractor employee for Coalescent Technology, which assists the National Guard Bureau at Fort Indiantown Gap, Pennsylvania. He remains in contact with (b)(6) and he does send her "adult content" e-mail, which he personally does not categorize as pornographic. Though not reflected in (b)(6) written notes, (b)(6) indicated he uses three computers at work, with at least one of these being his personal computer. (b)(6) did not remember ever using government computers to send "adult content" material to (b)(6) [Tab 6, Exhibit F, Notes from meeting between (b)(6) 1-7]. However, (b)(6) acknowledged using his AKO account to send suggestive e-mails to (b)(6) many

---

investigation regarding property accountability, her search was in furtherance of an investigation related to workplace misconduct. Technically, (b)(6) [redacted] servicing Systems Administrator should have conducted the search himself rather than giving the hard drive to Ms. Ahrens to retrieve for the documents and information she sought [*See* AR 25-2, paras 4-5s(10)(b)2, 4-5t, and 4-5t(5)]. Although this is a technical violation of AR 25-2, it is harmless. Nevertheless, Ms. Ahrens's direct, personal action to review (b)(6) hard drive is likely what prompted CID's and (b)(6) initial concerns.

times during duty hours [Tab 6, Exhibit F, Printed e-mail messages and images, pp. 11, 24, 30-38, 48-94].

The investigations uncovered no evidence that (b)(6) is or ever was a member of the armed forces, a Federal employee, or a Federal contractor employee [Tab 6, Exhibit U, Memorandum for Record of (b)(6)].

(b)(6) admitted to having personal photographs, mainly of her family, on her government computer. She also stated that, in the past, she had forwarded e-mails that she knows she should not have forwarded. (b)(6) asserted that she did not believe she had ever downloaded on the computer, but that she may not have been aware of doing so because she is not computer savvy. (b)(6) advised that she was sorry if she had done anything wrong, but asserted her belief that she simply did not understand. She apologized for forwarding inappropriate e-mails and indicated she would not do so in the future [Tab 6, Exhibit V, Statement of (b)(6) pp. 1-3]. Both [redacted]s discovery and (b)(6) investigation revealed numerous sexually explicit and other inappropriate e-mails forwarded and received by (b)(6) on her government computer during regular duty hours [Tab 6, Exhibit F, Printed e-mail messages and images, pp. 1-107].

**Findings:**

**OSC Allegation 1:** The allegation that Federal employees and contractors sent e-mails containing sexually explicit and inappropriate photographs and jokes, humor of a sexual nature, discussions of an obscene nature, and other inappropriate material from government e-mail accounts during duty hours, in violation of AR 25-1 and AR 25-2, is substantiated. Specifically—

**Allegation 1A:** The allegation that Federal employee, (b)(6) and contractor, (b)(6) sent e-mails from government e-mail accounts, containing explicit pornographic images is substantiated. E-mails between the two confirm that (b)(6) sent more than one sexually explicit image, via e-mail, to (b)(6) (b)(6) and to others, and that (b)(6) forwarded sexually explicit photos, via e-mail to (b)(6), another Federal employee and to a Soldier (b)(6) (b)(6) [23] in 2005 and 2006, respectively.

**Allegation 1B:** The allegation that (b)(6) Federal employees (b)(6) (b)(6), contractor (b)(6) whose employment status remains undetermined, sent e-mails from government e-mail accounts containing jokes and humor of a sexual nature, discussions of sexual encounters between employees, and other inappropriate material, is substantiated. E-mail messages authored and/or exchanged among all of the persons named above are contained in an exhibit attached to the investigation. Further, although (b)(6) admitted to receiving,

[23] Although (b)(6) apparently received the sexually explicit images from (b)(6) there is no evidence that he transmitted these images to anyone. Thus, at this time, TRADOC has determined not to refer the information further.

but not to forwarding inappropriate e-mail, the investigation revealed e-mail authored by (b)(6) that is extremely sexually suggestive in that it hints strongly at one or more clandestine rendezvous for sexual purposes with (b)(6) Photographs of (b)(6) in various states of dress were recovered from the hard drive of (b)(6) old computer.

**Allegation 1C:** The allegation that (b)(6) appeared in various states of undress in photographs recovered from the hard drive of (b)(6) old computer is substantiated. The investigative record reflects numerous photographs of (b)(6) in various states of undress.

**OSC Allegation 2:** (b)(6) used (b)(6) and (b)(6) (b)(6) government CACs and passwords between October 2007 and January 2008, in violation of AR 25-2.

**Relevant Authorities:**

(1) AR 25-2, paragraph 4-5a(8) [Tab 4] prohibits, among other activities--

Sharing personal accounts and authenticators (passwords or PINs) . . . with any unauthorized individual.

(2) AR 25-2, paragraph 4-5s(9) [Tab 4] states:

With the exceptions of the SA/NA,[24] as identified below, Army personnel and contractors are prohibited from browsing or accessing other user's e-mail accounts.

**Discussion:**

The Army gives each employee a unique, biometric-based CAC card that serves as the "primary access credential" to that individual's government computer. The use of the CAC to access the computer also requires a password that also is unique to the employee [Tab 4, AR 25-2, para 4-12a]. Army regulations do provide an authorized method for granting and gaining access to another employee's e-mail account or workstation, but do not allow employees to share CACs or passwords [AR 25-2, paras 4-5a(8), 4-5s(9)]. AR 25-2 requires that any deviation from the policies it promulgates be approved by the proponent of this regulation, the Army Chief Information Officer/G-6.

[redacted] and (b)(6) (Federal employee, GS-12) saw (b)(6) using (b)(6) CAC and e-mail account numerous times. [redacted] specifically recalls having observed this conduct from September to December 2007. [redacted] and (b)(6) also observed (b)(6) using the CAC and e-mail account of (b)(6) (b)(6) (now a retired Federal employee). (b)(6) observed this behavior

[24] "SA" is the acronym for Systems Administrator; "NA" is acronym for Network Administrator. *See* Tab 4, AR 25-2, Glossary.

on numerous occasions and volunteered her belief that (b)(6) commonly left her CAC and a slip of paper on which her Personal Identification Number (PIN) (or password) was written in a specific spot in her cubicle when she was out of the office [Tab 6, Exhibit B, Statement of [redacted] 1, "UNAUTHORIZED USE OF CAC/PIN AND SHARING OF PERSONALLY ASSIGNED E-MAIL ACCOUNTS"; Exhibit D, Statement of (b)(6), pp. 1-2, para 5].

(b)(6) (Federal employee, GS-09) observed (b)(6) using (b)(6) (b)(6) CAC on one occasion, but believes it was warranted because (b)(6) had been out of the office and had requested that (b)(6) use the CAC to perform work on (b)(6) computer to meet a suspense [Tab 6, Exhibit C, Statement of (b)(6) (b)(6) p. 1, para 1].

(b)(6) admits that she may have used (b)(6) CACs and computers while both were present in the office, and that she may have used (b)(6) computer to send e-mail when he was not present. However, she explained that the CAC use was intended to aid and complete the mission, as necessary, and in furtherance of office business, and not to injure the government. She stated that she often typed on computers while (b)(6) brainstormed, simply because she ((b)(6)) was the fastest typist. (b)(6) further explained that some of her use of the (b)(6) CAC and password may have occurred while (b)(6) was out of the office with serious medical problems [Tab 6, Exhibit V, Statement of (b)(6) pp. 1-3, paras 1-5].

**Findings:**

**OSC Allegation 2:** The allegation that (b)(6) used (b)(6) (b)(6) government CACs and passwords between October 2007 and January 2008 is substantiated. Witnesses conclusively state they observed (b)(6) using the CACs of others and accessing their computers, which access presumably would also have required that (b)(6) use the others' passwords. (b)(6) admitted that she likely engaged in this behavior. Although (b)(6) as supported by the testimony of (b)(6) asserted that she used others' CACs and passwords only in furtherance of mission completion and office business, (b)(6) actions nevertheless constituted a violation of AR 25-2. There is a formal process pursuant to which an authorized user of a government computer system may grant another user access to the first user's e-mail and computer files for workplace-related purposes. The informal sharing of CACs and passwords is strictly prohibited, however.

## COLLATERAL ISSUES

In his memorandum appointing (b)(6) as an IO under provisions of AR 15-6 to investigate the OSC-referred allegations, MG Turner additionally directed (b)(6) (b)(6) to make findings and appropriate conclusions concerning whether there existed any systemic shortfalls or mismanagement that allowed any misconduct found to occur

undetected until [redacted] discovered and reported it [Tab 6c, p. 2, paras 3a-c]. In response to this expanded tasking, (b)(6) made the following additional findings [Tab 6a]--

(1) TRADOC asserts that no systemic shortfalls were determined to have allowed or encouraged the misconduct and that both the Fort Eustis Directorate of Information Management (DOIM) and the ATSC information technology staff strictly adhere to AR 25-1 and AR 25-2. In this case, however, the DOIM did not discern any improper computer use by (b)(6) [Tab M, Statement of (b)(6) Information Assurance Manager, Fort Eustis, DOIM]. This is not unusual. (b)(6) determined that Fort Eustis DOIM adhered to Army protocols, as set forth in Army regulations [Tab 6, Exhibit O, Declaration of (b)(6); Exhibit P, Statement of (b)(6) p. 1].

(2) In his role as the Chief, VTT and (b)(6) supervisor, (b)(6) created a work environment that facilitated the misconduct addressed in the OSC-referred allegations by not enforcing the regulatory requirements of AR 25-1 and AR 25-2. (b)(6) (b)(6) also permitted inappropriate conduct to occur and personally contributed to the improper environment in the workplace. This finding is supported by evidence of record.

(b)(6) one of the witnesses interviewed by (b)(6), described the environment in the work unit supervised by (b)(6) very negatively and believed it was totally unacceptable. She considered him to have been an "ineffectual supervisor . . . [d]ue to his actions and his inaction, it is extremely difficult to respect him." [Tab D, Statement of (b)(6), p. 3, para 5]. Her own observations as well as (b)(6) disclosures to her caused (b)(6) to believe that (b)(6) (b)(6) engaged in a lengthy sexual affair [Tab 6, Exhibit D, Statement of (b)(6) pp. 1-3, paras 2-3, 8-15; Exhibit E, Memorandum from (b)(6), dated 6 August 2008, pp. 1-3, paras 3-6, 8-11, 13-14].

(b)(6) stated that both (b)(6) and [redacted] advised him of their concerns about (b)(6) inappropriate behavior. He requested that they proceed to address their concerns "with their own interventions" so he could keep the matter at arm's length in case he ultimately was called on to serve as a deciding or adjudicating official in an administrative action against (b)(6) [Tab 6, Exhibit K, Memorandum Statement of (b)(6), p. 1, para 1].

(b)(6) failed to provide effective leadership when the underlying conduct addressed in the OSC-referred allegations was brought to his attention. When initially informed of Ms. Ahrens's allegations, (b)(6) chose to focus primarily on Ms. Ahrens's actions leading to her discovery of the sexually explicit and other inappropriate materials on (b)(6) computer hard drive, not on the alleged violations of AR 25-1 and AR 25-2 by (b)(6) and others [Tab 6, Exhibit B, Statement of Ms. Sheila Ahrens; Exhibit I, Statement of (b)(6) Exhibit J, Statement of (b)(6) (b)(6); and Exhibit K, Memorandum Statement of (b)(6). The IO concluded that this initial focus on the individual making the report, [redacted], "created

the perception that management tolerated the inappropriate conduct and would not effectively deal with complaints concerning that conduct. . . . This created the perception among some employees that management approved of the inappropriate conduct and would resent efforts to correct it." [Tab 6a, para IIId].

## LISTING OF VIOLATIONS OR APPARENT VIOLATIONS OF LAW, RULE, OR REGULATIONS

**As to Allegation 1:** That Federal employees and contractors sent e-mails containing sexually explicit and inappropriate photographs and jokes, humor of a sexual nature, discussion of an obscene nature, and other inappropriate material from government e-mail accounts during duty hours violated AR 25-1 and AR 25-2. Although we acknowledge that some transmissions of pornography over the internet may be prohibited under criminal law as a violation of Title 18 USC, Section 1462, TRADOC did not address these OSC-referred allegations as a criminal matter. (b)(6) initially referred [redacted]s findings to the local CID detachment, but CID maintains a long standing policy of investigating only child pornography, and declined to investigate this case to the extent it involved only the transmission of adult pornography. Accordingly, the command investigated the allegations using administrative processes and, as warranted by the facts and circumstances of each individual case, imposed administrative sanctions against those determined to be responsible.

**As to Allegation 2:** Although (b)(6), as supported by the testimony of (b)(6) alleged that she used (b)(6) government CACs and passwords between October 2007 and January 2008, only in furtherance of mission completion and office business, (b)(6) actions constituted at least a technical violation of AR 25-2.

## CORRECTIVE ACTIONS

Disciplinary action was proposed to suspend (b)(6) from her duties at the ATSC, Fort Eustis, for a period of five days, for misuse of government property and resources, and for conduct unbecoming a federal employee [Tab F]. This is consistent with the recommendation of the AR 15-6 IO regarding (b)(6) Her grade, apparent remorsefulness, and lack of documented prior misconduct, as well as the command's treatment of similar offenses by other employees in the past, were considered in proposing this action. The suspension action was initiated and proposed by the Headquarters, TRADOC, Office of the Deputy Chief of Staff, G-3/5/7 to preclude any perceptions of bias by persons at ATSC. Subsequent to her receipt of the memorandum of proposed suspension, (b)(6) retired from Federal service on October 31, 2008 [Tab G].

Disciplinary action in the form of a written counseling statement has been issued to (b)(6) for his failure to provide effective and appropriate leadership, and to exercise sound judgment when issues related to the matters referred by OSC to the Army were initially presented to him [Tab H]. This action also is consistent with the recommendation of the AR 15-6 IO. The fact that (b)(6) did take action to investigate by referring the matter to CID, and investigated further by reviewing TDY vouchers to ascertain whether (b)(6) official travel coincided with that of (b)(6) (b)(6) was considered in taking action against (b)(6) Action against (b)(6) was taken by (b)(6) supervisor, the TRADOC Assistant Deputy Chief of Staff, G-3.

The evidence gathered in the context of this investigation was referred to (b)(6) (b)(6) second-level supervisor in the TRADOC Deputy Chief of Staff, G-3/5/7. While it does not appear that, (b)(6) routinely transmitted inappropriate e-mails or images on his computer, he did send an inappropriate e-mail to (b)(6) in 2003 using his government computer, during regular duty hours. Although the e-mail at issue is several years old, it was determined that (b)(6) status as a GS-13, coupled with his complete lack of total candor with the IO, merited counseling. Accordingly, (b)(6) issued a written counseling to (b)(6) [Tab I].[25]

Leades in the TRADOC Office of the Deputy Chief of Staff, G-3/5/7 have directed appropriate professional training from the Equal Employment Opportunity staff and others to ensure that both ATSC leadership and the workforce are aware of, and prepared to act on, Equal Employment Opportunity-related matters, as well as on other sensitive management issues in the workplace.

Leaders in the TRADOC Office of the Deputy Chief of Staff, G-3/5/7 also have directed a review of the ATSC supervisory structure and rating schemes to help ensure that all employees and managers are rated by appropriate supervisors, and that those supervisors are aware of their supervisory responsibilities.

Federal contractor employees are employed by the contractor performing a government contract and are obviously not Federal employees. Both (b)(6) (b)(6) are Federal contractor employees and have committed misconduct in the government workplace. (b)(6) exchanged more than one sexually explicit e-mail and other inappropriate materials with (b)(6) during duty hours. Further, regardless of whether he used his personal computer to do so, he clearly used his AKO account to transmit the e-mail. Although (b)(6) stated he does not recall receiving sexually explicit e-mail from (b)(6), he exchanged a number of sexually suggestive e-mails with her during duty hours.

---

[25] The IO also considered an allegation by (b)(6) that she "believed" (b)(6) had received a government laptop from (b)(6) for (b)(6) use. The IO did not pursue this allegation further because of a lack of specific information and an apparent lack of direct relevance to his investigation of the matters referred by OSC.

Accordingly, the results of this investigation were referred to the Adjutant General, State of Pennsylvania, Joint Forces Headquarters, Fort Indiantown Gap, Pennsylvania, to ensure that government contractor, Coalescent Technology, (b)(6) current employer, is aware of his misconduct and consideration is given to initiating appropriate action under the Coalescent Technology contract. The Adjutant General has advised TRADOC that (b)(6) contract expires in November 2008 and will not be renewed. Further, the results of the AR 15-6 investigation into the matters referred by OSC were referred to (b)(6) (b)(6) supervisor at Coalescent Technology for appropriate action **[Tab J]**.

The results of this investigation were provided also to legal counsel to the Contracting Officer at ATSC to ensure that (b)(6) employer, government contractor Wire One, is aware of his misconduct and consideration is given to appropriate action under the Wire One contract. Legal counsel determined that the misconduct occurred under a now-expired contract and ATSC was without a contractual remedy against (b)(6) or his employer. However, legal counsel will address (b)(6) conduct with the contractor to ensure that standards for the proper use of government equipment and e-mail usage are communicated to all contractor and subcontractor employees. Further, a report on this matter will be referred to the ATSC Security Manager so that he may notify the U.S. Army Central Personnel Clearance Facility, Fort Meade, Maryland, for appropriate action concerning (b)(6) security clearance.

Finally, AKO administrators will be notified of this misuse of government computers and of the AKO system so as to facilitate appropriate action concerning contractor employee misuse of AKO.

(b)(6) has retired from government service. (b)(6) clearly engaged in misconduct, exchanging numerous inappropriate e-mails with (b)(6) while employed at ATSC. However, as he is no longer a Federal employee, he cannot be disciplined for his misconduct.

Results of the investigation revealed that the employees discussed above probably engaged in sexual liaisons facilitated by their misuse of government computer systems and e-mail. One witness, (b)(6), alleged she was, on occasion, sent home early (at 3 o'clock or 4 o'clock P.M.) so that (b)(6) could spend time together **[Tab B, Statement of (b)(6), p. 3, para 1]**. However, there is no direct evidence that (b)(6) or any of the other subject employees or contractors engaged in this conduct during duty hours or at the duty site.

No evidence with national security implications has been disclosed in the context of this investigation.

## CLOSING COMMENTS

Federal employees must conduct themselves in a professional manner and refrain from using government resources and time for their own benefit. Further, they must not engage in conduct that tends to disgrace, discredit, or is in any way prejudicial to the Federal service in the conduct of its service to our nation.

The Army takes its responsibility to address concerns brought to it by the OSC very seriously. The Army has addressed the concerns raised in the instant allegations deliberately and thoughtfully. The planned corrective actions are intended to hold the responsible persons accountable and deter future, similar misconduct. Further, the additional training and reviews cited should help to ensure all employees are aware of their individual responsibilities and the Army's expectations for them.

This letter, with enclosures, is submitted in satisfaction of my responsibilities under Title 5, USC, Sections 1213 (c) and (d).

Sincerely,

21 Nov 09

Assistant Secretary of the Army
(Manpower & Reserve Affairs)

Army Report Documents

Tab A—The Secretary of the Army (SA) Delegation of Authority to the Assistant Secretary of the Army (Manpower &Reserve Affairs0 his authority, as agency head, to review, sign, and submit to Office of Special Counsel the report required by Title 5, USC, Sections 1213(b), (c) and (d), dated February 1, 2008

Tab B—OSC referral dated July 23, 2008 to the SA requesting he investigate allegations of violations of law, rule, or regulation; gross mismanagement; and a substantial and specific danger to public health and safety related activities at the U.S. Army Training Support Center (ATSC), Fort Eustis, Virginia

Tab C—Army Office of the General Counsel (OGC) forwarding memorandum of OSC request for investigation to U.S. Army Training and Doctrine Command for action, dated July 28, 2008

Tab D—Extension 1, requested September 22, 2008 (granted by OSC on September 23, 2008)

Tab E—Statement o [redacted] (b)(6), dated August 4, 2008

Tab F—Notice of Proposed Suspension [redacted] (b)(6) i, dated September 23, 2008

Tab G—Standard Form 50, Retirement c [redacted] (b)(6), effective date October 31, 2008

Tab H—Formal Counseling [redacted] (b)(6) ), dated September 23, 2008

Tab I—Formal Counseling [redacted] (b)(6) s, dated September 29, 2008

Tab J—Memorandum fron [redacted] (b)(6) n, Chief of Staff, Department of Military and Veterans Affairs, t [redacted] (b)(6) r, dated October 17, 2008

Tab K—Memorandum fron [redacted] (b)(6) <, Attorney, Mission and Installation Contracting Command, to Assistant Deputy Chief of Staff, G-3/5/7, regarding Results of AR 15-6 Investigation concerning contractor employe [redacted] (b)(6). [redacted] (b)(6) a, dated October 10, 2008

Tab L--CID Regulation 195-1,*Criminal Investigation Operational Procedures*, Chapter 13, Computer Crime and Electronic Evidence, para 13-8 (extract)

Tab M—Declaration c [redacted] (b)(6) n, dated November 26, 2008

Tab 1—Organizational Charts

Tab 2—Organizational Charts

Tab 3—Army Regulation 25-1, *Army Knowledge Management and Information Technology*, dated July 15, 2005

Tab 4—Army Regulation 25-2, *Information Assurance*, October 27, 2007

Tab 5—Appointment of Investigating Officer [redacted] (b)(6) |, August 4, 2008

Tab 6 (Tabs 6a-6d)—Report of Investigation- Findings and Recommendations of Investigating Officer, dated August 14, 2008

Tab 7—Staff Judge Advocate Legal Review of AR 15-6 Report, dated August 19, 2008

Tab 8—Staff Judge Advocate Transmission of AR 15-6 Report to MG Abraham Turner, Deputy Chief of Staff, G-3/5/7, Appointing Authority

Tab 9—Approval of AR 15-6 Report by MG Abraham Turner, Deputy Chief of Staff, G-3/5/7, Appointing Authority

# A

SECRETARY OF THE ARMY
WASHINGTON

FEB 01 2008

MEMORANDUM FOR ASSISTANT SECRETARY OF THE ARMY
(MANPOWER AND RESERVE AFFAIRS)

SUBJECT: Delegation of Authority Under Title 5, Sections 1213 (c) and (d)

In accordance with Title 10, United States Code, section 3013(f), I hereby delegate to you certain authority conferred upon me as agency head under Title 5, United States Code, section 1213. Specifically you are authorized to review, sign and submit written reports of investigations of information and related matters transmitted to the Department of the Army by The Special Counsel, in accordance with Title 5, United States Code, sections 1213(c) and (d). The authority delegated herein may not be further delegated.

This delegation shall remain in effect for three years from the date of its execution, unless earlier rescinded in writing by me.

Pete Geren

CF: General Counsel

Tab A

# B

U.S. OFFICE OF SPECIAL COUNSEL
1730 M Street, N.W., Suite 300
Washington, D.C. 20036-4505

The Special Counsel

July 23, 2008

The Honorable Preston M. Geren, III
Secretary
U.S. Department of the Army
1700 Army Pentagon
Washington, D.C. 20310-1700

Re: OSC File No. DI-08-2159

Dear Mr. Secretary:

Pursuant to my responsibilities as Special Counsel, I am referring to you a whistleblower disclosure that employees at the Department of the Army, Army Training Support Center (ATSC), Fort Eustis, Virginia, e-mailed pornography and obscene material from government e-mail accounts during official working hours. The whistleblower, [redacted] Division Chief, Human Performance Improvement Center, also alleged that employees shared passwords and Common Access Cards (cards). [redacted] who has consented to the release of her name, asserted that these activities constitute a violation of law, rule, or regulation. Accordingly, I am referring this information to you for an investigation of these allegations and a report of your findings.

The U.S. Office of Special Counsel (OSC) is authorized by law to receive disclosures of information from federal employees alleging violations of law, rule, or regulation, gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety. 5 U.S.C. § 1213(a) and (b). As Special Counsel, if I find, on the basis of the information disclosed, that there is a substantial likelihood that one of these conditions exists, I am required to advise the appropriate agency head of my findings, and the agency head is required to conduct an investigation of the allegations and prepare a report. 5 U.S.C. § 1213(c) and (g).

Specifically, [redacted] alleges that ATSC employees have been sending e-mails containing sexually explicit photographs and jokes, and conversations of an obscene nature from government e-mail accounts during official working hours. [redacted] submitted documents showing that Video Tele-Training Specialist [redacted] and contractor [redacted] have sent e-mails from government e-mail accounts containing explicit pornographic images. She also submitted documents revealing that [redacted], [redacted], TRADOC G357 employee [redacted], Educational Technology Team Chief [redacted] (now retired), contractor [redacted], and contractor [redacted] sent e-mails from government e-mail accounts containing jokes and humor of a

Tab B

sexual nature, discussions of sexual encounters between employees, and other inappropriate material. [redacted] further submitted home photographs of employees [redacted] and [redacted] showing both individuals in various states of undress. [redacted] found these e-mails and photographs on [redacted]'s work computer's hard drive. Copies of these documents are enclosed. [redacted] alleged that these actions violate Army Regulation 25-1, Army Knowledge Management and Information Technology, Chapter 6, Section 6-1f(1) (AR 25-1), and Army Regulation 25-2, Information Assurance, Chapter 4, Section 4-5r(7) (AR 25-2). AR 25-1 and AR 25-2 prohibit using Army communication systems for uses involving sexually explicit material such as pornography.

[redacted] also alleged that she witnessed [redacted] using Training Support Acquisition Specialist [redacted] (now retired) and [redacted] cards and computer passwords in violation of Army regulations between October 2007 and January 2008. [redacted] stated that the cards, which contain the picture of the employee, must be inserted into the computer before the system can be accessed. When inserted into the computer, the picture on the card is visible to individuals in the vicinity. [redacted] reported seeing [redacted] in [redacted] office using his computer and e-mail account. [redacted] stated that she could clearly see [redacted] card in the access slot. She also asserted that she has witnessed [redacted] using [redacted] computer with [redacted]'s card visible in the slot. [redacted] stated that [redacted] either would have had to know [redacted] and [redacted] passwords or been given access to the system by them in order to use their computers in this manner. [redacted] claimed that the unauthorized use of cards and passwords constitutes a violation of AR 25-2, Chapter 4, Sections 4-5a(8), and 4-5s(9). These sections, respectively, prohibit Army personnel and contractors from sharing passwords and accessing other users' e-mail accounts.

I have concluded that there is a substantial likelihood that the information provided by the whistleblower discloses a violation of law, rule, or regulation, including but not limited to, AR 25-1 and AR 25-2. As previously stated, I am referring this information to you for an investigation of these allegations and a report of your findings within 60 days of your receipt of this letter.

By law, the report must be reviewed and signed by you personally. Should you delegate your authority to review and sign the report to the Inspector General, or any other official, the delegation must be specifically stated and must include the authority to take the actions necessary under 5 U.S.C. § 1213(d)(5). Without this information, I would hasten to add that the report may be found deficient. The requirements of the report are set forth at 5 U.S.C. § 1213(c) and (d). A summary of § 1213(d) is enclosed. As a matter of policy, OSC also requires that your investigators interview the whistleblower as part of the agency investigation whenever the whistleblower consents to the disclosure of his name.

In the event it is not possible to report on the matter within the 60-day time limit under the statute, you may request in writing an extension of time not to exceed 60 days. Please be advised that an extension of time is normally not granted automatically, but only upon a showing of good cause. Accordingly, in the written request for an extension of time, please state specifically the reasons the additional time is needed. Any additional requests for an extension of time must be approved by me.

After making the determinations required by 5 U.S.C. § 1213(e)(2), copies of the report, along with any comments on the report from the whistleblower, and any comments or recommendations by this office will be sent to the President and the appropriate oversight committees in the Senate and House of Representatives. 5 U.S.C. § 1213(e)(3).

Unless classified or prohibited from release by law or by Executive Order requiring that the information be kept secret in the interest of national defense or the conduct of foreign affairs, a copy of the report and any comments will be placed in a public file in accordance with 5 U.S.C. § 1219(a).

Please refer to our file number in any correspondence on this matter. If you need further information, please contact Catherine A. McMullen, Chief, Disclosure Unit, at (202) 254-3604. I am also available for any questions you may have.

Sincerely,

Scott J. Bloch

Enclosures

Enclosure

Requirements of 5 U.S.C. § 1213(d)

Any report required under subsection (c) shall be reviewed and signed by the head of the agency[1] and shall include:

(1) a summary of the information with respect to which the investigation was initiated;

(2) a description of the conduct of the investigation;

(3) a summary of any evidence obtained from the investigation;

(4) a listing of any violation or apparent violation of law, rule or regulation; and

(5) a description of any action taken or planned as a result of the investigation, such as:

(A) changes in agency rules, regulations or practices;

(B) the restoration of any aggrieved employee;

(C) disciplinary action against any employee; and

(D) referral to the Attorney General of any evidence of criminal violation.

In addition, we are interested in learning of any dollar savings, or projected savings, and any management initiatives that may result from this review.

[1] Should you decide to delegate authority to another official to review and sign the report, your delegation must be specifically stated.

# C

DEPARTMENT OF THE ARMY
OFFICE OF THE GENERAL COUNSEL
104 ARMY PENTAGON
WASHINGTON DC 20310-0104

Suspense: September 5, 2008
July 28, 2008

MEMORANDUM THRU COL Donald Curry, Office of the Staff Judge Advocate, Headquarters Training and Doctrine Command, Building 10, Room 319, 11 Bernard Road, Fort Monroe, Virginia 23651-5000

MEMORANDUM FOR LTC Timothy Cody, Office of the Staff Judge Advocate, Headquarters U.S. Army Transportation Center & Fort Eustis, 2732 Madison Avenue, Fort Eustis, Virginia 23604-5026

SUBJECT: Whistleblower Investigation—U.S. Army Training Support Center (ATSC), Fort Eustis, Virginia (OSC File DI-08-2159)

Enclosed for your action is a July 23, 2008 letter from the Office of Special Counsel (OSC), requesting an investigation of the noted allegations and a report pursuant to 5 U.S.C.1213(c)(1) and (g).

The Special Counsel has concluded that there is substantial likelihood that information provided by a whistleblower, [redacted] with first-hand knowledge, discloses that there is a substantial likelihood that Department of the Army employees and contractor personnel at the Army Training Support Center (ATSC), Fort Eustis, Virginia, may have engaged in activities that violate a law, rule, or regulation, including, but not limited to Army Regulation25-1, Army Knowledge Management and Information Technology, and Army Regulation 25-2, Information Assurance.

Specifically, [redacted] alleges that these individuals emailed pornography and obscene material from government email accounts during official working hours. She alleges that ATSC personnel, [redacted] (Video Tele-Training Specialist), and contactor [redacted] have sent emails from government email accounts containing sexually explicit photographs, while [redacted], TRADOC G/3/5/7 employee [redacted], Educational Technology Team Chief [redacted] (now retired), contractor [redacted], and contractor [redacted], sent emails from government email accounts containing jokes and humor of a sexual nature, discussions of sexual encounters between employees, and other inappropriate material. [redacted] also submitted home photographs of employees [redacted] and [redacted] showing both individuals in various states of undress. [redacted] found these emails and photographs on [redacted] work computer's hard drive. Copies of these documents are enclosed. [redacted] alleged that these actions violated Army Regulation 25-1, Army Knowledge Management and Information Technology, Chapter 6, Section 6-1f(1), and Army

Tab S

Printed on Recycled Paper

Regulation 25-2, Information Assurance , Chapter 4, Section 4-5r(7). Both regulations prohibit using Army communication systems for uses involving sexually explicit material such as pornography.

Additionally [redacted] alleges that individuals shared passwords and Common Access Cards (CAC cards). [redacted]s alleges that she witnessed [redacted] using Training Support Acquisition Specialist [redacted] (now retired) and [redacted] cards and computer passwords in violation of Army Regulation 25-2, Chapter 4, Sections 4-5a(8) and 4-5s(9). These sections prohibit Army personnel and contractors from sharing passwords and accessing other users' email accounts.

A final response describing any actions taken to address the allegations should be prepared for the signature of the Assistant Secretary of the Army (Manpower and Reserve Affairs) (ASA (M&RA)) who has been delegated the authority by the Secretary of the Army to review, sign and submit written reports of investigations of information and related matters transmitted to the Department of the Army by the Special Counsel, in accordance with Title 5, United States Code (U.S.C.), § 1213(c), (d) and (g). The final response should be submitted to this office AS SOON AS POSSIBLE BUT NOT LATER THAN September 5, 2008.

The Army's response will be available to the public and information contained in the Army response will made public unless classified or prohibited from release by law or by Executive order requiring that information be kept secret in the interest of national defense or the conduct of foreign affairs. Therefore, our response and any supporting investigative report should be prepared in a manner intended to facilitate public understanding of the allegations and Army's response thereto.

The requirements specified in 5 U.S.C. § 1213(d) (copy enclosed) may be used as a guideline and should include findings, conclusions and corrective action. In all cases, please furnish for our review all backup materials supporting the proposed response that will be used to prepare the official response for the Secretary of the Army.

When you forward your report to me, please do so by providing two hard copies of the complete report, including all backup/supporting documentation. Additionally, by email to me, please provide the electronic version of the report, including the findings, conclusions and corrective action, but not the backup/supporting documentation. The electronic version will facilitate retrieving and incorporating as much of your draft report as possible directly into the final Army report. A sample report will be provided to you to use relative to the appropriate format, approach, and content that should serve as a pattern for your report.

Please note that should you encounter any problems with the inquiry/investigation and preparation of the subject report, kindly call me as soon as possible to discuss. In

some instances, ancillary issues that arise during the course of the investigation may require follow up action.

In conducting your investigation into the allegations, please ensure that the methods and process used are compatible with engaging in a fair and open "dialog" with the OSC regarding the subject allegations and that there are no restrictions or limitations placed on the use or disclosure of the information gathered and relied upon to support the final Army report.

Additionally, the potential use of your report to support any disciplinary actions against individuals based on misconduct should also be considered when structuring your investigation and preparing your report.

Lastly, note that copies of the final Army report, along with comments on the report from the individuals making the disclosures and any comments or recommendations by the OSC will be sent to the President and the appropriate oversight committees in the Senate and House of Representatives pursuant to 5 U.S.C. § 1213(e)(3). Additionally, the Army's final report and any comments to it will be made available to the public. Accordingly, please structure your report so that no restrictions or limitations are placed on its dissemination or the disclosure of the information upon which it relies.

By statute, the agency has sixty (60) days from receipt of the OSC letter to provide the required report. If necessary, I will seek an extension of the date for our reply to the Special Counsel. As soon as it becomes apparent that more time beyond the suspense noted above will be needed to complete your report, you should forward to me an interim response requesting the extension and indicating the reasons for the request and the date by which I can expect to receive your final response. As you can understand, once your report is forwarded to me, I will need additional time to staff the proposed response to the OSC and finalize the Army's report.

If you have any questions, please do not hesitate to contact me at [redacted] Additionally, my email address is [redacted]

[redacted]

Associate Deputy General Counsel
(Human Resources)

Enclosures

# D

DEPARTMENT OF THE ARMY
OFFICE OF THE GENERAL COUNSEL
104 ARMY PENTAGON
WASHINGTON DC 20310-0104

September 22, 2008

Ms. Catherine A. McMullen
Chief, Disclosure Unit
U.S. Office of Special Counsel
1730 M Street, N.W., Suite 300
Washington, D.C. 20036-4505

Re: OSC File No. DI-08-2159

Dear Ms. McMullen:

This letter is a status report for the above captioned case. I am requesting that you grant an extension of time to file the Department of the Army's report required by 5 USC § 1213 for the above captioned Office of Special Counsel (OSC) case where OSC determined that there is substantial likelihood that information provided by a whistleblower, [redacted] with first-hand knowledge, discloses that there is a substantial likelihood Department of the Army employees and contractor personnel at the Army Training Support Center (ATSC), Fort Eustis, Virginia, may have engaged in activities that violate a law, rule, or regulation, including, but not limited to Army Regulation 25-1, Army Knowledge Management and Information Technology, and Army Regulation 25-2, Information Assurance.

Specifically, [redacted] alleges that these individuals emailed pornography and obscene material from government email accounts during official working hours. She alleges that ATSC personnel, [redacted] (Video Tele-Training Specialist), and contactor [redacted] have sent emails from government email accounts containing sexually explicit photographs, while [redacted], TRADOC G/3/5/7 employee [redacted], Educational Technology Team Chief [redacted]s (now retired), contractor [redacted], and contractor [redacted], sent emails from government email accounts containing jokes and humor of a sexual nature, discussions of sexual encounters between employees, and other inappropriate material. [redacted] also submitted home photographs of employees [redacted] and [redacted] showing both individuals in various states of undress. [redacted] found these emails and photographs on [redacted]'s work computer's hard drive. Copies of these documents are enclosed. [redacted] alleged that these actions violated Army Regulation 25-1, Army Knowledge Management and Information Technology, Chapter 6, Section 6-1f(1), and Army Regulation 25-2, Information Assurance , Chapter 4, Section 4-5r(7). Both regulations prohibit using Army communication systems for uses involving sexually explicit material such as pornography.

Additionally, [redacted] alleges that individuals shared passwords and Common Access Cards (CAC cards). [redacted] alleges that she witnessed [redacted] using Training Support Acquisition Specialist [redacted]y (now retired) and [redacted]

Tab D

Printed on Recycled Paper

[redacted] cards and computer passwords in violation of Army Regulation 25-2, Chapter 4, Sections 4-5a(8) and 4-5s(9). These sections prohibit Army personnel and contractors from sharing passwords and accessing other users' email accounts.

I respectfully submit the following status report and further request that you grant the Department of the Army an additional extension of time to file its report in this matter. This extension will permit the Army to complete some additional inquiries that surfaced during its recent investigation into the OSC referred allegations, and finalize its final Army report for transmission to OSC in satisfactions of the 5 USC §1213 report. To date, the following actions have been taken on this case.

On July 28, 2008, I forwarded the OSC correspondence for appropriate action to the United States Army Training and Doctrine Command (TRADOC), Headquarters, Office of the Staff Judge Advocate (OSJA) for action. COL Donald Curry advised the command group about the allegations. In turn, on August 4, 2008, Major General (MG) Abraham Turner, the TRADOC Deputy Chief of Staff G-3/5/7, appointed [redacted] as an Investigating Officer, under the provisions of AR 15-6, Procedures for Investigating Officers and Boards of Officers, to conduct an informal investigation into the allegations of misconduct made by [redacted]s. TRADOC completed its investigation and prepared a draft Army report based on the AR 15-6 investigation report. On September 4, 2008, COL Curry forwarded both documents to my office for our review. A review of these documents indicated that there were several areas of inquiry that remained to be developed. A teleconference was held on September 22, 2008 to address these outstanding matters.

Therefore, this request for an extension is being made in order to complete that supplemental investigation and allow sufficient time for the TRADOC OSJA to review the investigation, prepare and staff the draft Army report , and then forward it to OGC for further staffing and completion of the final Department of the Army report in satisfaction of the 5 USC § 1213 requirements.

Should you grant this extension, please advise me as to the length of the extension. Within that allotted time, I will either provide you another status update on this pending action or be able to submit the final Department of the Army report to the Special Counsel.

I appreciate your assistance in considering the extension request. To advise me if this extension will be granted, you can reach me at [redacted]

[redacted]

Associate Deputy General Counsel
(Human Resources)

# E

# DECLARATION

Pursuant to 28 U.S.C. Section 1746, I, Colonel John B. Halstead, make the following declaration.

1. I possess a Ph.D. in Systems and Information Engineering from the University of Virginia, and I have significant contributions in the field within peer-reviewed publications. I consider myself a data mining expert.

2. On 4 August 2008 I was appointed as an AR 15-6 Investigating Officer to investigate misconduct by Federal employees and contractor employees at Army Training Support Center (ATSC), Fort Eustis, Virginia. I completed my investigation on or about 14 August 2008.

3. During the course of my investigation, I reviewed [redacted] current (as of August 2008) e-mail folders and found previously undiscovered additional images and movies that were sexually explicit and inappropriate (included on discs in my investigation). I am aware [redacted]s and [redacted], ATSC employees who reviewed the contents of [redacted] computer in May 2008, did not discover that material. I conclude that they did not find everything I found because the additional material was added after they reviewed the e-mail folders in May, or because my advanced academic training enabled me to discover that material.

Tab E

I declare under penalty of perjury that the foregoing is true and correct. Executed on November 7, 2008.

John B. Halstead
Colonel, U.S. Army

# F

DEPARTMENT OF THE ARMY
HEADQUARTERS UNITED STATES ARMY TRAINING AND DOCTRINE COMMAND
102 MCNAIR DRIVE
FORT MONROE VIRGINIA 23651-1047

REPLY TO
ATTENTION OF

ATTG-ZC

23 September 2008

MEMORANDUM FOR [redacted], U.S. Army Training Support Center, ITSD, Training Support Services Division, Fort Eustis, VA 23604

SUBJECT: Notice of Proposed Suspension

1. This memorandum is official notification that I am proposing to suspend you from your position without pay for five (5) calendar days for conduct unbecoming a civilian employee and misuse of a government computer. This proposed action is being taken in accordance with Title 5, United States Code, Chapter 75 (5 USC, Section 7501 and following); Title 5 Code of Federal Regulations, Part 752 (5 CFR 752) and Army Regulation (AR) 690-700, Chapter 751, and is for such cause as to promote the efficiency of the service .

2. The specific reasons supporting this proposed action are as follows:

a. From at least 2002 through 2006, you used your government computer to repeatedly transmit lewd, pornographic or sexually explicit e-mail notes and images to several Federal employees, contractor employees, and at least one Soldier during duty hours.

b. You maintained and transmitted pornographic or sexually explicit images and videos on the hard drive of your government computer.

c. During at least September to December 2007, you used the computer access cards (CACs) of other Federal employees, and accessed the e-mail accounts of those employees.

3. Your repeated and multiple lewd messages, the pornographic or sexually explicit files on your computer hard drive, and your improper use of other employees' CACs



Tab F

and e-mail accounts were verified and examined by an investigating officer pursuant to AR 15-6. Copies of his report, including his findings and recommendations and the material found on the websites and your hard drive, were made available to me for review during deliberations on this proposal.

4. Your conduct in transmitting lewd, sexually explicit or pornographic messages and images during duty hours and on your government computer was conduct unbecoming a Federal employee. It was wrong, and tended to disgrace and discredit the Federal service. In fact, your misconduct was discovered inadvertently by another Federal employee who promptly reported it.

5. Misuse of your government computer under the circumstances of your conduct is a violation of:

a. Department of Defense Regulation 5500.7-R, Joint Ethics Regulations, Chapter 2 (Standard of Ethical Conduct), Section 2-301 (Use of Government Resources).

b. AR 25-1, Army Knowledge Management and Information Technology, paragraph 6-1f(1).

c. AR 25-2, Information Assurance, paragraphs 4-5a(8), 4-5r(7), and 4-5s(9).

6. By virtue of your many years of government experience and evidence of you taking and passing your annual information technology assurance examination in January 2008, you were aware or should have been aware that viewing, transmitting, and maintaining of sexually explicit or pornographic material on your computer is a violation of numerous policies and regulations, to include those listed above.

7. In proposing this suspension, I have considered the nature and seriousness of these type offenses and your position as an experienced employee in a position requiring independent work and trust, as well as your past work record and the absence of any disciplinary actions in your record. I also considered your past work performance and your potential for future work and rehabilitation. It is your responsibility to adhere to Army and government policies and regulations regarding computer use. The volume

of improper materials on your government computer was substantial, and your viewing and transmitting of sexually explicit materials was intentional and occurred over a lengthy period, wasting government time and possibly affecting your ability to accomplish your duties satisfactorily. The introduction of sexually explicit material into the workplace creates a debilitating and potentially discriminatory work environment, and its presence inherently impedes the full inclusion of all employees as professional equals. Further, while there is no direct evidence that you had inappropriate sexual liaisons with your former supervisor and other Federal employees through your Federal employment and with the aid of government computers, many of the e-mails you exchanged contain circumstantial evidence of this misconduct. Your improper conduct reflected poorly on yourself and your organization, and casts a negative image on the Department of the Army.

8. Comparing your offenses to the Table of Penalties, Table 1-1, AR 690-700, Chapter 751, the range of disciplinary actions for a first offense of Misuse of Government Property is a written reprimand to removal from Federal service. The range of actions for a first offense of Conduct Unbecoming a Federal Employee is a 1-day suspension to removal from the Federal service. A proposed suspension of five (5) calendar days is the minimum disciplinary measure necessary for you to correct your behavior. This proposed action is to maintain good order and discipline and to correct your conduct. This action, if sustained by the deciding official, will not take effect any earlier than ten (10) calendar days from the day you receive this proposal notice.

9. You may respond to this notice of proposed suspension orally, in writing, or both stating why this proposed suspension action should not be taken. Your reply, if any, should be made to me, [redacted], Assistant Deputy Chief of Staff, G-3/5/7, Headquarters, U.S. Army Training and Doctrine Command, Fort Monroe, and must be within fourteen (14) calendar days from the date you receive this letter. You may present witnesses and/or furnish affidavits and other documentary evidence in support of your response. Consideration will be given to extending this period if you submit a request stating your reasons for desiring more time.

10. You have the right to elect a representative to assist you in preparing and presenting a reply to this proposal. You may elect anyone you wish as long as the representational activities of the individual chosen will not cause a conflict of interest or position, or give rise to unreasonable costs to the U.S. Government. Any choice of or change in representative must be designated in writing and include your representative's name, address and a telephone number. This designation must be signed and dated by your representative and submitted to me as the deciding official.

11. You are entitled to a reasonable amount of official time during your normal tour of duty to review the material relied upon to support the reasons for this notice, for preparing a written reply, for securing affidavits and statements of witnesses in support of your answer, and for making an oral reply, should you desire. You must contact [redacted], Deputy to the Assistant Deputy Chief of Staff, G-3/5/7, (757) 788-5797, in advance, to make arrangements for the use of official time.

12. Full consideration will be given to any reply, affidavits, or other evidence you submit before a final decision is rendered. Whether or not you make a reply, a decision will be rendered after the expiration of the period allowed for your answer. I will notify you in writing of my decision. You will remain in a duty status during the notice period of this proposed action.

13. If you believe that your unacceptable conduct may be caused by personal, physical, or medical problems; substance abuse; and/or other reasons not directly related to the duties of your position, you are advised and strongly encouraged to use the assistance of the Employee Assistance Program at Fort Eustis. This program is designed to assist employees with personal problems and refer them to sources within the community that offer treatment or rehabilitative care. For additional information regarding this service, contact the Civilian Counseling Service at (757) 878-1487.

14. You and/or your representative may review the material relied upon to support this action, to include applicable Department of the Army regulations by calling [redacted]

ATTG-ZC
SUBJECT: Proposed Suspension

[redacted] Office of the Staff Judge Advocate, Building 10, Room 319, Fort Monroe, VA 23651-1111, telephone (757) 788-4186.

ROBERT E. SEGER
Senior Executive Service
Assistant Deputy Chief
of Staff, G-3/5/7

CF:
Fort Eustis CPAC

ACKNOWLEDGEMENT OF RECEIPT [redacted]
DATE: 9/23/08

# G

Standard Form 50-B
Rev. 7/91
U.S. Office of Personnel Management

# NOTIFICATION OF PERSONNEL ACTION

| 1. Name (Last, First, Middle) | 2. Social Security Number | 3. Date of Birth | 4. Effective Date |
|---|---|---|---|
| [redacted] | [redacted] | [redacted] | 10-31-2008 |

| FIRST ACTION | | SECOND ACTION | |
|---|---|---|---|
| 5-A. Code: 303 | 5-B. Nature of Action: Retirement-Special Option | 6-A. Code | 6-B. Nature of Action |
| 5-C. Code: USM | 5-D. Legal Authority: 5 U.S.C. 9902(g) | 6-C. Code | 6-D. Legal Authority |
| 5-E. Code | 5-F. Legal Authority | 6-E. Code | 6-F. Legal Authority |

**7. FROM: Position Title and Number**
VIDEO TELETRAINING SITE SPECIALIST
141216 - 824634

| 8. Pay Plan | 9. Occ. Code | 10. Grade/Level | 11. Step/Rate | 12. Total Salary | 13. Pay Basis |
|---|---|---|---|---|---|
| GS | 0301 | 09 | 04 | $49,546.00 | PA |

| 12A. Basic Pay | 12B. Locality Adj. | 12C. Adj. Basic Pay | 12D. Other Pay |
|---|---|---|---|
| $43,776.00 | $5,770.00 | $49,546.00 | |

**14. Name and Location of Position's Organization**
US ARMY TRAINING SUPPORT CENTER
USATSC, ITSD
TRAINING SUPPORT SVCS DIV
FORT EUSTIS, VA 23604 57GC

**15. TO: Position Title and Number**

| 16. Pay Plan | 17. Occ. Code | 18. Grade/Level | 19. Step/Rate | 20. Total Salary/Award | 21. Pay Basis |
|---|---|---|---|---|---|
| | | | | | |

| 20A. Basic Pay | 20B. Locality Adj. | 20C. Adj. Basic Pay | 20D. Other Pay |
|---|---|---|---|
| | | | |

**22. Name and Location of Position's Organization**

## EMPLOYEE DATA

| 23. Veterans Preference | 24. Tenure | 25. Agency Use | 26. Veterans Preference for RIF |
|---|---|---|---|
| 1 (1 - None; 2 - 5-Point; 3 - 10-Point/Disability; 4 - 10-Point/Compensable; 5 - 10-Point/Other; 6 - 10-Point/Compensable/30%) | 1 (0 - None; 1 - Permanent; 2 - Conditional; 3 - Indefinite) | | YES: [ ] NO: [X] |

| 27. FEGLI | 28. Annuitant Indicator | 29. Pay Rate Determinant |
|---|---|---|
| C0 Basic only | 9 Not Applicable | 0 |

| 30. Retirement Plan | 31. Service Comp. Date (Leave) | 32. Work Schedule | 33. Part-Time Hours Per Biweekly Pay Period |
|---|---|---|---|
| K FERS and FICA | 04-08-1987 | F Full-Time | |

## POSITION DATA

| 34. Position Occupied | 35. FLSA Category | 36. Appropriation Code | 37. Bargaining Unit Status |
|---|---|---|---|
| 1 (1 - Competitive Service; 2 - Excepted Service; 3 - SES General; 4 - SES Career Reserved) | E (E - Exempt; N - Nonexempt) | [redacted] | AR5813 |

| 38. Duty Station Code | 39. Duty Station (City - County - State or Overseas Location) |
|---|---|
| 511004700 | FORT EUSTIS / NEWPORT NEWS / VIRGINIA |

| 40. Agency Data | 41. | 42. | 43. | 44. |
|---|---|---|---|---|
| | PON# OA | | | TDA DATA TC/W3E9AA/822G/099 |

45. Remarks

Forwarding address: 232 Saddler Drive, Newport News, VA 23608-2621.

Reason for retirement: to obtain retirement benefits.

Lump-sum payment to be made for any unused annual leave.

| 46. Employing Department or Agency | | | 50. Signature/Authentication and Title of Approving Official |
|---|---|---|---|
| U.S. Army Training and Doctrine Command (ARTC) | | | FeRosario Arquero-Ashley<br>AUTHORIZING OFFICIAL |
| 47. Agency Code: ARTC | 48. Personnel Office ID: 1991 | 49. Approval Date: 10-17-2008 | |

Tab G

5-Part 50-316

TURN OVER FOR IMPORTANT INFORMATION

Editions Prior to 7/91 Are Not Usable After 6/30/93
NSN 7540-01-333-6238

# H

DEPARTMENT OF THE ARMY
HEADQUARTERS UNITED STATES ARMY TRAINING AND DOCTRINE COMMAND
102 MCNAIR DRIVE
FORT MONROE VIRGINIA 23651-1047

REPLY TO
ATTENTION OF

ATTG-ZC

23 September 2008

MEMORANDUM FOR [redacted], Executive Director, Army Training Support Center, Deputy Chief, G/3/5/7, U.S. Army Training and Doctrine Command, Fort Eustis, VA 23

SUBJECT: Formal Counseling

1. The purpose of this memorandum is to express my concern that you did not fully and effectively discharge your supervisory responsibilities regarding recent events within Army Training Support Center (ATSC). Specifically, you failed to thoroughly address misconduct by employees involving misuse of government computers for personal, inappropriate, and lewd purposes, and you did not address the underlying concerns of at least one employee who brought this to your attention. Unfortunately, your focus was misguided in that you directed much of your scrutiny in the matter at the person who reported the misconduct rather than actual wrongdoers. As a result, that person perceived that you were more interested in punishing her than those responsible for the conduct itself, causing her to lose confidence in her local leadership and report the matter to higher authorities. Based on evidence gathered during subsequent investigation, her reaction to discussions with you on this topic were reasonable.

2. I am aware that you did investigate or cause to be investigated certain potential criminal aspects of the misconduct, and that you did direct your deputy to investigate the underlying misconduct. However, you did not fully inform the person who brought this to your attention of these facts, and you exercised extremely poor judgment by creating the perception you cared more about discovering any possible wrongdoing by that person than those who committed the actual violations. This demonstrates insensitivity to important workplace dynamics and the overall working environment.

3. Your significant Federal government experience and your previously unblemished record lead me to conclude that this written counseling is sufficient to correct the judgmental deficiencies noted above. However, I fully expect you to

Tab
4

exercise sound judgment and display the requisite workplace sensitivities to resolve any future issues or problems arising within your activity. Any failure to act consistently with my expectations may subject you to further action.

4. To assist in correcting deficiencies and discharging managerial responsibilities at ATSC, I plan to schedule ethics and Equal Employment Opportunity-related training for employees there. Representatives from this headquarters will contact you concerning scheduling of this training.

ROBERT SEGER
Senior Executive Service
Assistant Deputy
Chief of Staff, G-3/5/7

Receipt acknowledged.

[redacted]

23 Sep 08
Date

ATTG-TRC September 2008

MEMORANDUM FOR [redacted], Distributed Learning Directorate, Deputy Chief of Staff, G/3/5/7, U.S. Army Training and Doctrine Command, Fort Monroe, VA 23651

SUBJECT: Formal Counseling

1. The purpose of this memorandum is to express my concerns that you fail to understand your duties and responsibilities as a senior Federal employee. Specifically, you engaged in misconduct and demonstrated poor judgment in communicating with another Federal employee in a personal, inappropriate, and sexually suggestive manner through use of a government computer during duty hours in 2003. Recently, you also were less than candid with an officer appointed to investigate the discovery of a substantial number of inappropriate and sexually suggestive e-mail messages and images when you were questioned about your possible involvement in the matter. You acknowledged receiving "adult explicit material" from [redacted] but indicated you deleted and did not forward it. While that much may be true, you did not acknowledge that you had authored and sent the inappropriate message referenced above.

2. Your significant Federal government experience and your previously unblemished record lead me to conclude that this written counseling is sufficient to correct the deficiencies noted above. However, I fully expect you to exercise sound judgment and ensure that your future conduct does not violate Army policy or the norms expected of Federal employees. Any failure to act consistently with my expectations may subject you to further action.

ROBERT C. MORRIS
Colonel, GS
Director, dLD

Receipt acknowledged: [redacted]

Date: 29 Sep 08

Tab I

J

DEPARTMENT OF MILITARY AND VETERANS AFFAIRS
ADJUTANT GENERAL'S OFFICE
**COMMONWEALTH OF PENNSYLVANIA**
FORT INDIANTOWN GAP
ANNVILLE, PENNSYLVANIA 17003-5002
VOICE/TDD 1-800-645-8924
www.dmva.state.pa.us

COS

17 October 2008

MEMORANDUM FOR TRADOC, ATTN: ATTG-ZC, [redacted]

SUBJECT: Results of AR 15-6 Investigation

1. [redacted]s a Coalescent Contractor on Fort Indiantown Gap.

2. His contract expires in November 2008 and will not be renewed.

3. The 15-6 investigation was forwarded to his supervisor at Coalescent Technology, Mr. Micah Nordquist (407) 691-7966, for him to take action, since it is out of my jurisdiction.

FOR THE ADJUTANT GENERAL:

BARRY T. LOWEN
Col, PaANG
Chief of Staff

CF:
[redacted]

# K

DEPARTMENT OF THE ARMY
MISSION AND INSTALLATION CONTRACTING COMMAND
MICC CENTER – FORT EUSTIS
2798 HARRISON LOOP
FORT EUSTIS, VA 23604-5538

REPLY TO
ATTENTION OF

SFCA-MICC-L

10 October 2008

MEMORANDUM FOR Assistant Deputy Chief of Staff, G-3/5/7, HQ U.S. Army TRADOC, ATTN: [redacted], OSJA, TRADOC, 102 McNair Drive, Ft. Monroe, VA 23651-1047

SUBJECT: Results of AR 15-6 Investigation

1. This office has reviewed the results of the investigation conducted pursuant to AR 15-6 into the misconduct of Federal employees and Federal contractor employees at the U.S. Army Training Support Center (ATSC), Ft. Eustis, VA. The investigating officer concluded that a contractor employee, [redacted] performing work under a contract at the ATSC, committed misconduct when he exchanged inappropriate and sexually suggestive material with [redacted] (a Government employee) during duty hours. The report was forwarded to the MICC-Center for consideration and referral to Wire One for appropriate action pertaining to the Wire One employee.

2. The services were performed under a now expired contract with Sprint. The Contracting Officer could not confirm whether Wire One was a subcontractor under that contract. Performance under the current contract commenced in October 2006. The conduct investigated and deemed inappropriate, took place between August 2005 and March 2006, i.e. under the predecessor contract, but was not discovered until May 2008. No performance issues were reported under the contract during the period of August 2005 and March 2006 that relate to [redacted]

3. As the inappropriate conduct took place under a now expired contract, no contractual remedy exists. Furthermore, even if that contract were still in existence, as no performance issues resulted from [redacted] conduct, the issue was not raised until 2 years after the conduct took place, and the Contractor has performed satisfactory to date, no reason exist to ask the Contractor to remove [redacted] from performance under the Contract. To do so would result in a liability to the Government for any cost related to replacing [redacted] and could lead to affect performance under the contract for the period required to replace [redacted] with someone equally qualified.

4. This office will address [redacted] conduct with the Contractor and request that the Contractor communicates the proper use of Government IT equipment and e-mail usage to all its employees and any subcontractor employees working under the Contract. The Government has no direct contractual relationship with any subcontractors and as such can only address any performance issues with the Contractor. Any further action where subcontractors and/or contractor personnel are concerned will be at the Contractor's discretion.

Tal K

5. POC is the undersigned at [redacted] or at [redacted]

[redacted]

Attorney, Office of Counsel
MICC Center - Fort Eustis

L

[redacted] OGC

**From:** [redacted] Ms OGC
**Sent:** Tuesday, November 25, 2008 4:30 PM
**To:** [redacted] OGC
**Subject:** FW: CIC Policy (UNCLASSIFIED)

**Importance:** High

**Attachments:** Chapter 13-8.doc

Chapter 13-8.doc
(27 KB)


[redacted]
Department of the Army
Office of the General Counsel
104 Army Pentagon Room 3C546
Washington D.C. 20310-0104
[redacted] (office)
[redacted] (fax)


-----Original Message-----
From: [redacted] T LTC MIL USA USACIDC
Sent: Tuesday, November 25, 2008 4:23 PM
To: [redacted] F Ms OGC
Subject: RE: CIC Policy (UNCLASSIFIED)
Importance: High

Classification: UNCLASSIFIED
Caveats: NONE

Carrie, Attached is the chapter of CIDR 195-1 that contains our policy regarding investigation of pornography. If you have any questions please let me know.

Vr,


[redacted]
[redacted]
Staff Judge Advocate
U.S. Army Criminal Investigation Command (USACIDC)
[redacted]



ATTORNEY CONFIDENTIALITY NOTICE - LAW ENFORCEMENT SENSITIVE - This e-mail and any accompanying attachments may include information that constitutes attorney work product and/or client advice, which is legally privileged. It may also contain information that is further privileged because of its Law Enforcement Sensitive nature. This information should not be released to unauthorized persons, and should be maintained in a separate file. If you are not the intended recipient of this information any disclosure, copying, distribution, or the taking of any action in reliance on this information is prohibited. If you received this e-mail in error, please notify the sender immediately by calling (703) 806-3383 or by return e-mail.


Tab L

**Title:** Criminal Investigation Operational Procedures
**Authors:** U.S. Army Criminal Investigation Command
**Document Number:** CID Regulation 195-1
**Build Date:** 4 April 2008 **Version:** 8

## CHAPTER 13
## COMPUTER CRIME AND ELECTRONIC EVIDENCE

### 13-8. Child Pornography, Adult Pornography and Other Obscene Matter

a. Title 18 USC, Sections 2251-2260, Sexual Exploitation and other Abuse of Children and Title 18 USC, Section 1460-1470, Obscenity, make it a federal offense to possess, distribute, import or transport (including by mail, common carrier or the use of a computer) what is commonly referred to as child and adult pornography (hereafter referred to as "prohibited images"). Child pornography is broadly defined as a visual depiction of a person under the age of eighteen engaging in sexually explicit conduct as defined in Title 18, Section 2256. The CID will not normally conduct investigations pertaining to adult pornography and other obscene matter when it is the only offense or in conjunction with another offense not normally within the investigative purview of CID.

# M

## DECLARATION

Pursuant to 28 U.S.C. Section 1746, I, [redacted], make the following declaration.

1. I am the Information Assurance Manager employed at the Fort Eustis Directorate of Information Management (DOIM) with four years experience in information management.

2. I am aware that Army Regulation (AR) 25-2, paragraph 3-3, requires information assurance training in order for all Army and contractor employees to be issued network access. The training requirement is an annual one and, to the best of my knowledge, all employees at Fort Eustis perform this annual training.

3. I am also familiar with the ability of the Fort Eustis DOIM staff and systems to manage the contents of employees' computers. While there is a management tool able to discover inappropriate content on government computers, Fort Eustis does not have the ability to routinely monitor or scan personal e-mails and their contents sent or received on those computers. Ability to conduct such monitoring for inappropriate content is limited by resources and regulation (AR 380-53, Conduct of Information Security Monitoring) and is only authorized in support of Law Enforcement, Counterintelligence, and Management searches as outlined in AR 25-2, pg 23, Para 4-5, t thru u.

Therefore, it is possible for employees to send and receive inappropriate or sexually explicit to other employees without being subjected to normal detection.

4. The Fort Eustis DOIM adheres to the information assurance requirements of AR 25-2 and follows all protocols.

I declare under penalty of perjury that the foregoing is true and correct. Executed on November 26, 2008.

[redacted]
Information Assurance Manager

[redacted] E-Signed by [redacted] 083523596 [redacted] 10

## CLOSING COMMENTS

Federal employees must conduct themselves in a professional manner and refrain from using government resources and time for their own benefit. Further, they must not engage in conduct that tends to disgrace, discredit, or is in any way prejudicial to the Federal service in the conduct of its service to our nation.

The Army takes its responsibility to address concerns brought to it by the OSC very seriously. The Army has addressed the concerns raised in the instant allegations deliberately and thoughtfully. The planned corrective actions are intended to hold the responsible persons accountable and deter future, similar misconduct. Further, the additional training and reviews cited should help to ensure all employees are aware of their individual responsibilities and the Army's expectations for them.

This letter, with enclosures, is submitted in satisfaction of my responsibilities under Title 5, USC, Sections 1213 (c) and (d).

Sincerely,

21 Nov 08

Assistant Secretary of the Army
(Manpower & Reserve Affairs)

The Honorable Scott J. Bloch
The Special Counsel
U.S. Office of Special Counsel
1730 M Street, N.W., Suite 300
Washington, D.C. 20036-4505

RE: Whistleblower Investigation – U.S. Army Training Support Center (ATSC), Fort Eustis, Virginia (OSC File DI-08-2159)

Dear [redacted]:

In accordance with Title 5, United States Code (USC) Sections 1213 (c) and (d), the enclosed report is submitted in response to your referral of information requesting an investigation of allegations and a report of findings in the above-referenced case.

As the Agency head, the Secretary of the Army (SA) has delegated to me his authority to review, sign, and submit to you the report required by Title 5, USC, Sections 1213(b), (c) and (d) (Tab 1).

Note that this report and its exhibits contain the names and duty titles of employees, Soldiers, and contractor employees of the Army Training Support Center (ATSC) and Headquarters, U.S. Army Training and Doctrine Command (TRADOC), Fort Monroe, Virginia, as well as sexually explicit and inappropriate photographs and e-mails. Subsequent release of this information may result in violations of the Privacy Act,[1] and breaches of personal privacy interests. Accordingly, those releases required by Title 5, USC, Section 1213(e) excepted, the Department of the Army requests the opportunity to coordinate in advance on any release of this report outside the Office of Special Counsel.

## INFORMATION INITIATING THE INVESTIGATION

By letter dated July 23, 2008, the OSC referred to the SA its conclusion that information provided by a whistleblower with first-hand knowledge , [redacted], discloses that there is a substantial likelihood that Department of the Army employees and contractor personnel at the ATSC, Fort Eustis, Virginia[2], may have engaged in

[1] The Privacy Act of 1974 is codified at Title 5, USC, Section 552a.
[2] Organization charts of Headquarters, TRADOC, the Deputy Chief of Staff, G-3/5/7, and ATSC are at Tab 2.

activities that violate a law, rule, or regulation, including, but not limited to Army Regulation (AR) 25-1, Army Knowledge Management and Information Technology, (Tab 3) and AR 25-2, Information Assurance (Tab 4).

Specifically, [redacted] alleges the following:

(1) Based on her discovery of emails and photographs on the hard drive of [redacted] government computer,

(a) [redacted] ATSC Video Teletraining Specialist, and [redacted] contractor employee at the ATSC, have sent e-mails containing sexually explicit photographs from government email accounts;

(b) [redacted] Headquarters, TRADOC, Deputy Chief of Staff G-3/5/7, employee, [redacted] former (now retired) ATSC Educational Technology Team Chief, contractor employee [redacted], and contractor employee [redacted] sent emails from government email accounts containing jokes, humor of a sexual nature, discussions of sexual encounters between employees, and other inappropriate material; and

(c) [redacted] and [redacted] appeared in various states of undress in photographs on the hard drive.

The above actions violate AR 25-1, paragraph 6-1f(1), and AR 25-2, paragraph 4-5r(7).

(2) She has witnessed [redacted], and [redacted] former (now retired) ATSC Training Support Acquisition Specialist, sharing computer passwords and Common Access Cards (CAC), in violation of AR 25-2, paragraphs 4-5a(8) and 4-5s(9).

## CONDUCT OF THE INVESTIGATION

By statute, an agency is afforded sixty days to complete the report required by Title 5, USC, Section 1213. On July 28, 2008, the Office of Army General Counsel (OGC) forwarded the OSC request for investigation through the Office of the Staff Judge Advocate (OSJA), Headquarters, TRADOC, to the Office of the Staff Judge Advocate, Fort Eustis, for action. ATSC, while physically located at Fort Eustis, is an operating agency of Headquarters, TRADOC, Deputy Chief of Staff G-3/5/7, located at Fort Monroe. Therefore, because an investigation into potential misconduct at ATSC and any subsequent corrective action would likely be taken at Headquarters, TRADOC, it is most appropriate that OSJA, Headquarters, TRADOC, assume responsibility for legal oversight in this case.

On August 4, 2008, Major General (MG) Abraham Turner, the TRADOC Deputy Chief of Staff G-3/5/7, appointed Colonel [redacted] as an Investigating

Officer (IO) under the provisions of AR 15-6, Procedures for Investigating Officers and Boards of Officers, to conduct an informal investigation into the allegations of misconduct made by [redacted] (Tab 5). Specifically, MG Turner appointed [redacted] investigate the allegations that Federal employees [redacted], [redacted] and [redacted] (now retired), and contractor employees [redacted], and [redacted] used government equipment and/or resources to transmit inappropriate email messages and photos to other employees, and to investigate whether any of the named employees improperly shared passwords and accessed other users' email accounts, in violation of AR 25-1 and AR 25-2. MG Turner further tasked [redacted] to ascertain whether there was any systemic problem or any mismanagement which aided the misconduct or allowed it to occur undetected. Finally, [redacted] was directed to investigate and report on any additional violations of law, rule, or regulation he discovered by any persons during the course of his investigation into the allegations of [redacted].

During his investigation, as memorialized in the Report of Investigation (ROI) (Tab 6), [redacted] gathered documentary evidence in the form of emails and photographic attachments sent to and among Federal and contractor employees, primarily at ATSC, Fort Eustis. He also interviewed 17 persons associated with the allegations, including key witnesses [redacted], [redacted], [redacted], [redacted], [redacted], the Director, ATSC, and [redacted] (Tab 6, Exhibits (Ex.) V, S, R, Q, T, K, B, respectively). As a result of those interviews, he obtained 13 sworn statements, four "official" memorandums of record, one certified email statement, and records of his conversations with [redacted] and [redacted].

On August 14, 2008, [redacted] completed his findings and recommendations, and submitted his ROI to the Headquarters, TRADOC OSJA for legal review, as his legal advisor instructed. [redacted] found that:

(1) [redacted] improperly used government equipment to transmit sexually explicit and inappropriate material, and this violated AR 25-1, paragraph 6-1f(1)[3], and AR 25-2, paragraph 4-5r(7)[4];

(2) he could not determine whether [redacted] (contractor) used a government computer or his personal computer to transmit inappropriate and sexually explicit material because he used both types of computer in his office;[5]

---

[3] This provision prohibits "Use of communications systems that would adversely reflect on DOD or the Army (such as uses involving sexually explicit e-mail or access to sexually explicit Web sites, pornographic images, or virtual computer-generated or otherwise pornographic images)."

[4] This provision prohibits "any personal use of Government resources involving: pornography or obscene material (adult or child);...."

[5] [redacted] stated he has sent [redacted] "adult-content" images, but denied sending anything pornographic and, to the best of his memory, has never sent her "adult-content" images on AKO or government systems (Tab 6, Ex. T, Notes from a meeting between [redacted], IO, and [redacted] "[redacted], numbers 4) and 6) ).

(3) no evidence indicates [redacted], [redacted], or [redacted] ansmitted sexually explicit or inappropriate material;

(4) no evidence indicates [redacted] is or was a member of the armed forces, a Federal employee, or a Federal contractor employee (Tab 6, Ex. U, Statement of Clay A. Brashear);

(5) [redacted] ri, [redacted] and [redacted] improperly shared computer access cards ("CAC" cards) and passwords, in violation of AR 25-2, paragraph 4-5a(8);[6]

(6) [redacted] improperly accessed [redacted] and [redacted] email accounts, in violation of AR 25-2, paragraph 4-5s(9);[7]

(7) No systemic problems or shortfalls allowed or encouraged the misconduct, as both the Fort Eustis Directorate of Information Management (DOIM) and the ATSC's information technology staff strictly adhere to AR 25-1 and AR 25-2, and executed procedures and systems that enforce employee compliance;

(8) [redacted] as the former Chief, Video Tele-Training, and [redacted] former supervisor, created a work environment that permitted the misconduct by not enforcing AR 25-1 and AR 25-2 requirements;

(9) [redacted] s tolerated an environment that permitted inappropriate conduct and contributed to the current environment within the Video Tele-Training Branch; and

(10) [redacted] the Director, ATSC, failed to provide effective leadership in addressing these issues when they were brought to his attention by focusing on the reporting person ([redacted]) rather than the underlying violations, thereby creating a perception that management tolerated the inappropriate conduct and would not effectively deal with complaints concerning that conduct.

As a result, COL Halstead recommended:

(1) [redacted] s supervisors take appropriate remedial and disciplinary action against her for violations of AR 25-1 and AR 25-2;

(2) [redacted] supervisors take appropriate remedial and disciplinary action to address his failure to exercise appropriate leadership and use sound judgment in his attempts to resolve the issues identified in this investigation when they were made known to him in May 2008;

(3) ATSC leaders receive appropriate professional training designed to enhance their

---

[6] This provision prohibits "[s]haring personal accounts and authenticators (passwords or PINs) … with any unauthorized individual."

[7] This provision prohibits, with exceptions not applicable here, Army personnel and contractors "from browsing or accessing other user's e-mail accounts."

ability to effectively lead their organization and to appropriately respond to Equal Employment Opportunity issues; and

(4) Headquarters, TRADOC, Deputy Chief of Staff, G-3/5/7 leaders review the ATSC supervisory structure and rating schemes to ensure all employees and managers are supervised and rated appropriately and fairly.

On August 19, 2008, Major Linda A. Chapman, Chief, Military Law Division, OSJA, TRADOC, completed a legal review of the investigation and determined that the proceedings complied with the legal requirements, there were no appointing or substantial errors, the evidence was sufficient to support the IO's findings, and the recommendations were consistent with the findings (Tab 7 ). On August 21, 2008, [redacted], Acting SJA, TRADOC, endorsed [redacted] legal review and determined that the investigation was legally sufficient. He recommended that the appointing authority, MG Turner, approve the investigating officer's findings and recommendations (Tab 8). MG Turner approved the findings and recommendations on August 26, 2008 (Tab 9).

## SUMMARY OF EVIDENCE OBTAINED FROM THE INVESTIGATION

The evidence regarding the allegations that Government and contractor employees improperly used Army communications systems for purposes involving transmission of sexually explicit material, and that Government employees improperly shared passwords and accessed other users' e-mail accounts is summarized below.

**OSC Allegation 1. Federal employees and contractors have been sending e-mails containing sexually explicit photographs and jokes, and conversations of an obscene nature from government e-mail accounts during duty hours, in violation of AR 25-1 and AR 25-2.**

**a) Federal employee [redacted] and contractor [redacted] have sent e-mails from government e-mail accounts containing explicit pornographic images;**

**b) [redacted] Federal employees [redacted] (retired) and [redacted], and contractor employees [redacted] and [redacted], have sent e-mails from government e-mail accounts containing jokes and humor of a sexual nature, discussions of sexual encounters between employees, and other inappropriate material.**

**OSC Allegation 2. [redacted] used Federal employee [redacted] (retired) and [redacted] access cards and computer passwords between October 2007 and January 2008, in violation of AR 25-2.**

1. Relevant Authorities:

a. OSC Allegation 1.

(1) AR 25-1, Army Knowledge Management and Information Technology, July 25, 2005, establishes Army policies and assigns responsibilities for the management of information resources and information technology. AR 25-1, Chapter 6, concerns command, control, and computer technology support and services. Paragraph 6-1f(1) states the following prohibition:

> Use of communications systems that would adversely reflect on DOD or the Army (such as uses involving sexually explicit e-mail or access to sexually explicit Web sites, pornographic images, or virtual computer-generated or otherwise pornographic images);....and other uses that are incompatible with public service.

(2) AR 25-2, Information Assurance, October 24, 2007, establishes information assurance policy, roles, and responsibilities. AR 25-2, Chapter 4, addresses information assurance policy. Paragraph 4-5r(7) indicates:

> Certain activities are never authorized on Army networks. AUP[8]s will include the following minimums as prohibited. These activities include any personal use of Government resources involving: pornography or obscene material (adult or child;...

b. OSC Allegation 2.

(1) AR 25-2, paragraph 4-5a(8) prohibits, among several other actions:

> **Sharing personal accounts and authenticators (passwords or PINs)...with any unauthorized individual** (emphasis in original).

(2) AR 25-2, paragraph 4-5s(9) states:

> **With the exceptions of the SA/NA[9] as identified below, Army personnel and contractors are prohibited from browsing or accessing other user's e-mail accounts** (emphasis in original).

2. Discussion:

[redacted] began his investigation on August 4, 2008, and ascertained the following facts.

a. OSC Allegation 1.

(1) On April 30, 2008, [redacted], a contractor employee at ATSC, conducted a life cycle replacement of the government computer formerly used by [redacted]

---

[8] "AUP" denotes "Authorized Use Policy." See AR 25-2, Glossary.
[9] "SA" is the Systems Administrator; "NA" is the Network Administrator. See AR 25-2, Glossary.

(Federal employee, GS-09) at the Fort Eustis activity. Pursuant to ATSC procedure, he asked M[redacted]s former second-level supervisor, [redacted] (Federal employee, YA-03), if she needed any of the data remaining on that computer. [redacted] wanted to retain historical knowledge of the VideoTele-Training and the Satellite Education Network programs, so she requested [redacted] transfer the hard drive's data to the shared portal. As [redacted] had difficulty transferring the hard drive data, he removed the hard drive and gave it to [redacted] (Tab 6, Ex. A, Statement of [redacted], p. 1; Ex. B, Statement of [redacted]s, p. 2, "DISCOVERY").

(2) [redacted] also attempted to obtain historical files by coordinating with [redacted]s new supervisors, [redacted]l (a now retired Federal employee) and [redacted] Federal employee, YA-03) (Tab 6, Ex. B, Statement of [redacted]s, p. 1, "SPECIAL DETAIL"; p. 2, "DISCOVERY"). When Ms. Canevari transferred from the Video Tele-Training program to Training Support Services Division (TSSD) Operations, [redacted]s "re-ghosted"[10] [redacted] new computer within TSSD Operations and transferred her former Video Tele-Training and Satellite Education Network files to her new computer on or about February 12, 2008 (Tab 6, Ex. A, Statement of [redacted]s, p. 1). As of May 13, 2008, [redacted] had not received all of the historical files requested through coordination, and [redacted] had not transferred the Satellite Education Network files (Tab 6, Ex. B, Statement of [redacted], p. 2, "DISCOVERY").

(3) [redacted] took her government laptop computer and the hard drive from [redacted] former computer to her ([redacted] home to continue working on May 14, 2008 (Tab 6, Ex. B, Statement of [redacted] p. 2, "DISCOVERY"; N, Statement of David Ahrens, p. 1). [redacted]s, [redacted] husband and a Federal employee, assisted her in connecting the hard drive to the laptop. As she was able to read the hard drive, she began searching it and downloading relevant Video Tele-Training and Satellite Education Network files. [redacted]s discovered sexually explicit and other inappropriate images and PowerPoint presentations within e-mail folders, which [redacted]ad e-mailed to Soldiers, Federal employees, and Federal contractor employees. She consolidated her discoveries and gave them to V[redacted] ATSC Deputy Director, (YC-03) on or about May 19, 2008 (Tab 6, Ex. B, Statement of [redacted] p. 2, "DISCOVERY"; Ex. F, e-mail messages and images, pp. 1-107; Ex. G, Statement of [redacted] pp. 2-3, paragraph 3b).

(4) The discoveries contained inappropriate images of [redacted] (Federal employee, GS-13) in undergarments; sexually explicit images and materials attached to e-mail sent to [redacted]s and [redacted] (Federal contractor), dated September 12, 2006; sexually explicit material sent to [redacted] etired Federal employee), dated June 5, 2006; sexually explicit material sent to Army Sergeant [redacted], dated June 2, 2006; an inappropriate image attached to e-mail sent to [redacted]s, [redacted] and [redacted], dated March 9, 2006; sexually explicit material in a PowerPoint presentation attached to e-mail sent to [redacted], dated December 9, 2005; and

[10] "Re-ghosting", or "re-imaging", is the process of purging unwanted or, in this case, inappropriate files and data from a computer while leaving the remaining files intact.

inappropriate images attached to e-mail sent to numerous recipients, dated November 2, 2005. There was also sexually explicit material attached to incoming e-mail received by [redacted] from [redacted], dated December 9, 2005, and June 2 and 5, 2006 (Tab 6, Ex. F, Printed e-mail messages and images, pp. 1-107).

(5) [redacted] delivered the images and PowerPoint presentations provided by [redacted] to [redacted] (Federal employee, YC-03) on or about May 20, 2008. He in turn consulted the Army Criminal Investigation Division (CID) at Fort Eustis, as well as the ATSC Support Directorate for guidance (Tab 6, Ex. K, Statement of [redacted], p. 1, paragraph 2; Ex. L, Statement of [redacted]. On the advice of these technical staffs, [redacted] instructed the Support Directorate to seize the removed hard drive, [redacted] computer, [redacted]' old computer, and [redacted] new computer on May 22, 2008 (Tab 6, Ex. B, Statement of [redacted], p. 3, "DISCOVERY", paragraph 3; Ex. G, Memorandum of [redacted] p. 3, paragraph 3d; Ex. K, Statement of [redacted], p. 1, paragraph 3; Ex. L, Statement of [redacted] p. 1). Army CID personnel informed [redacted] that [redacted] actions in making her discovery on [redacted] old computer may have been improper and may warrant a "hand slap" (Tab 6, Ex. K, Statement of [redacted], p. 1, paragraph 3a). However, CID would only become involved if child pornography was discovered on the hard drive or any of the computers, and no child pornography was found (Tab 6, Ex. K, Statement of [redacted] p. 1, paragraph 3b). [redacted] informed his superior of the foregoing on or about May 23, 2008 (Tab 6, Ex. K, Statement of [redacted], p. 2, paragraph 4).

(6) On May 27, 2008, [redacted] hosted a meeting with Sergeant Major (SGM) [redacted], [redacted], and [redacted], with the understanding among the latter three that they would discuss the way ahead regarding [redacted]' discovery (Tab 6, Ex. B, Statement of [redacted], p. 3, paragraph 4; Ex. I, Statement of [redacted], p. 1, paragraphs 1, 2; Ex. J, E-mail narrative of IO, adopted by SGM [redacted], p. 1, paragraphs 4, 5). However, [redacted] focused the discussion primarily on a single email string among [redacted] and himself[11] and on [redacted] questionable method of discovery; he failed to address the organization's response to [redacted] possible misuse of government equipment in transmitting inappropriate and sexually explicit email. [redacted] also read the Table of Penalties for employee misconduct[12] to [redacted] (Tab 6, Ex. B, Statement of [redacted] p. 3, 4, "DISCOVERY", paragraphs 4-6; Ex. I, Statement of [redacted], p. 1, paragraphs 4-6; Ex. J, E-mail narrative adopted by SGM [redacted], paragraphs 5, 6). SGM [redacted] believes [redacted] not only failed to address the issue, but failed to understand command responsibilities regarding [redacted] discovery (Tab 6, Ex. J, E-mail narrative adopted by SGM [redacted] paragraph 8).

(7) On June 3, 2008, [redacted] received two directives from his supervisor. First pursue appropriate action against ATSC employees with pornography on a government computer; second, determine whether there was any indication [redacted] had used

---

[11] The email exchange between [redacted] and [redacted] on December 13, 2004, concerned a holiday potluck for ATSC personnel (Tab 6, Ex. F, p. 46)

[12] AR 690-700, Chapter 751, Table 1-1, Table of Penalties for Various Offenses.

government travel to facilitate or further any sexual liaisons with other employees or government contractors. [redacted]o tasked his deputy, [redacted]es, with the first action after the ATSC Support Directorate provided the scan results on July 3, 2008.[13] Concerning the second directive, [redacted]o personally reviewed [redacted] temporary duty (TDY) records from December 2002 through February 2007, then had the (dLD) Director review [redacted] TDY records for the same period. A comparison of the two record sets found no TDY correlation. He determined that the two employees did not improperly use government funds for personal reasons (Tab 6, Ex. K, Statement of [redacted], p.2, paragraphs 4-6).

(8) As [redacted] had not informed [redacted] that he had directed [redacted] investigate the inappropriate material on [redacted]s old computer, [redacted]s solicited the help of her husband, [redacted], to use the "open door" policy of Mr. [redacted]r, Senior Executive Service, TRADOC Deputy G-3 ([redacted]s supervisor), to bring this matter to his attention. [redacted] resented his spouse's concerns to [redacted], [redacted] deputy (YA-03), although he did not provide any documentary evidence. [redacted] then consulted [redacted]la, TRADOC OSJA Labor Counselor, and on that counsel he informed [redacted] of the general situation without compromising his potential decision making authority , because he did not discuss specifics. [redacted]r offered [redacted]s the opportunity of an office call to provide physical evidence and firsthand knowledge, but she declined. [redacted] informed [redacted] she could use the "open door" policy, but advised against it because she would potentially require [redacted] as a decision authority in the matter (Tab 6, Ex. B, Statement of [redacted] p. 4, "DISCOVERY", paragraph 2; Ex. M, Statement of [redacted]. 1; Ex. N, Statement of [redacted] pp. 1, 2).

(9) At the direction of his supervisor, [redacted] (Federal employee, ATSC, GS-12) and [redacted] (Federal employee, ATSC) reviewed the content of [redacted] current computer in early May 2008. They did find inappropriate images attached to e-mails sent from her computer to other e-mail recipients, but did not discover any additional sexually explicit material on the computer. Further, they did not find any sexually explicit material or inappropriate images on [redacted]' old and new

---

[13] [redacted] informal investigation into this matter is reflected in his Memorandum for Record of July 22, 2008 (Tab 6, Ex. G, Memorandum of [redacted] and his memorandum to the IO on August 7, 2008 (Tab 6, Ex. H, Memorandum of [redacted]). There is no further record of this investigation. [redacted] also reference a previous AR 15-6 investigation in which [redacted] was the IO (Tab 6, Ex. B, Statement of [redacted] pp. 1,2, "SPECIAL DETAIL", "DISCOVERY", paragraph 3; Ex. D, Statement of [redacted] p. 2, paragraph 7; Ex. G, Memorandum of [redacted] pp. 1,2, paragraph 2 ). That investigation concerned property accountability issues for which an AR 15-6 investigation was appropriate under AR 735-5, Policies and Procedures for Property Accountability, paragraph 13-25, and it is not relevant to the issues central to this report, but [redacted] was involved in assisting the IO. [redacted] reference yet another informal investigation, this by [redacted] in January 2008 into alleged inappropriate office behavior. [redacted] retired in April 2008. Her investigation was self-initiated and, although she did interview some persons, no findings or recommendations were ever reduced to writing; however, it did result in a sensing session and a transfer of [redacted] another position (Tab 6, Ex. B, Statement of [redacted]. 2, paragraph 1; Ex. D, Statement of [redacted] p. 3, paragraphs 1, 3; Ex. G, Memorandum of [redacted] 2, 5, paragraphs 2b, 5 ).

computers, or on [redacted] computer (Tab 6, Ex. L, Statement of [redacted], p. 1; Ex. G, Memorandum of [redacted]s, Enclosures 3, 4).

(10) [redacted] the IO, reviewed [redacted]'s e-mail folders and discovered additional sexually explicit inappropriate images and movies within them, primarily within her sent and deleted folders. The images included personal sexually explicit images (Tab 6, Ex. X, disc).[14] His discovery also included all of the images and PowerPoint presentations found by [redacted] (Tab 6, Ex. X, disc). His review determined that [redacted]'s files were dominated by legitimate government work, and the sexually explicit images were sporadic. The images from [redacted]i's saved e-mail files are consolidated on five compact discs (Tab 6 , Ex. Y, discs).

(11) [redacted]s concluded and [redacted] specifically found that [redacted] acting in her supervisory role, could examine the hard drive on [redacted]'s old government computer for relevant historical files, and to assist another IO in a property accountability investigation (Tab 6; see also, Tab 6, Ex. G, Memorandum of [redacted] encl 4). Therefore, [redacted]' actions regarding [redacted]'s old computer were substantively proper in the execution of her supervisory responsibilities, in accordance with AR 25-2, paragraph 4-5a(7).[15]

(12) [redacted]s, the only Federal employee referenced in this investigation not performing duties at ATSC, acknowledged receiving "adult explicit material" from [redacted]i in the past, but states he deletes it and does not forward it (Tab 6, Ex. R, Statement of [redacted]s, p. 1). However, [redacted] authored one lengthy message to [redacted] in the e-mail discovered by [redacted]. The message is dated November 4, 2003, at 1:19 PM, sent with an Army e-mail address, and is clearly suggestive in nature (Tab 6, Ex. F, Printed e-mail messages and images, p. 10).

(13) [redacted] (retired Federal employee), refused to provide a statement to the IO, but did emphasize that he did not understand the allegations regarding [redacted]. He referred to her as a "churchgoing woman" and a "loving grandmother" (Tab 6, Ex. S, Notes from meeting between [redacted] and [redacted], 1-4). There are a significant number of suggestive e-mail message exchanges between him and [redacted] during 2002, 2005, and 2006, almost all of which were during duty hours (Tab 6, Ex. F, Printed e-mail messages and images, pp. 11-22).

---

[14] [redacted]'s discovery is admittedly inconsistent with [redacted] review (discussed in the paragraph immediately preceding) in that [redacted] found more information and images than [redacted]. The probable explanation is that [redacted] possesses a Ph.D. in Systems and Information Engineering, and is a data mining expert, and he therefore was better able to discover the additional material (Addendum, enclosure 1).

[15] [redacted] should have requested that her servicing Systems Administrator obtain any and all necessary information as part of a management search to enable her to perform her duties, rather than obtain it personally and directly. See AR 25-2, paragraph 4-5s(10)(b)2. Her failure to fully comply with this requirement is likely what concerned both CID and [redacted] even though she had authority as a supervisor to eventually access the information.

(14) [redacted] Federal contractor employee at ATSC), did not recall receiving sexually explicit e-mail from [redacted] He does delete and does not forward any inappropriate email he receives (Tab 6, Ex. Q, Statement of [redacted] p. 1). However, there are a number of e-mail message exchanges between him and [redacted] [redacted] the majority of which are during duty hours and are extremely suggestive in nature (Tab 6, Ex. F, Printed e-mail messages and images, pp. 95-99, 101-107 ).

(15) [redacted] is a contractor employee for Coalescent Technology, which assists the National Guard Bureau at Fort Indiantown Gap, Pennsylvania. He remains in contact with [redacted] and he does send her "adult content" e-mail, which he personally does not categorize as pornographic. Though not reflected in [redacted]'s written notes, [redacted] indicated he uses three computers at work, and at least one of them is a personal computer. He did not remember ever using government computers to send adult content material to [redacted] (Tab 6, Ex. F, Notes from meeting between [redacted] O, and [redacted], 1-7). However, he did use his Army Knowledge Online (AKO) account to send suggestive e-mails to [redacted] many times during duty hours (Tab 6, Ex. F, Printed e-mail messages and images, pp. 11, 24, 30-38, 48-94).

(16) There is no record of [redacted] ever being a Federal employee, a Federal contractor employee, or a member of the armed services (Tab 6, Ex. U, Memorandum for Record of Clay A. Brashear).

(17) [redacted] admitted to having personal photographs, mainly family photos, on her computer. She also stated she forwarded e-mails that she knows she should not have in the past. She does not believe she ever downloaded on the computer, but she may not have known if she did because she is not computer savvy. If she did anything wrong, she is sorry, but she believes she simply did not understand. She apologized for forwarding inappropriate emails and indicated she would not do so in the future (Tab 6, Ex. V, Statement of [redacted], pp. 1-3). Both [redacted] discovery and [redacted] investigation revealed numerous inappropriate and sexually explicit e-mails forwarded and received by her on her government computer during duty hours (Tab 6, Ex. F, Printed e-mail messages and images, pp. 1-107).

b. OSC Allegation 2.

(1) [redacted] and [redacted] (Federal employee, GS-12) saw [redacted] using [redacted] CAC and e-mail account numerous times. [redacted] observed it specifically from September to December 2007. [redacted] and [redacted] also observed [redacted] using the CAC and e-mail account of [redacted] (a retired Federal employee). [redacted] observed this numerous times, and volunteered that [redacted] left her CAC and a slip of paper with her Personal Identification Number in a specific spot in her cubicle when she was out of the office (Tab 6, Ex. B, Statement of [redacted] p. 1, "UNAUTHORIZED USE OF CAC/PIN AND SHARING OF PERSONALLY ASSIGNED EMAIL ACCOUNTS"; Ex. D, Statement of [redacted] pp. 1-2, paragraph 5).

(2) [redacted]vis (Federal employee, GS-09) observed [redacted] using [redacted]s CAC on one occasion, but believes it was warranted because [redacted] was out of the office and requested [redacted] use the card to meet a suspense (Tab 6 , Ex. C, Statement of [redacted] p. 1, paragraph 1).

(3) [redacted] admits that she may have used [redacted] and [redacted] CACs and computers while both were present, and that she may have used [redacted] computer to send e-mail when he was not present. However, she explained that the CAC use was intended to aid and complete the mission when necessary in order to complete office business, not to injure the government. She stated that she often typed on computers while [redacted]s and [redacted] brainstormed, as she was the fastest typist. She further explained that some of this may have occurred while [redacted] was out of the office with serious medical problems (Tab 6, Ex. V, Statement of [redacted] pp. 1-3, paragraphs 1-5).

c. Additional Relevant Evidence.

(1) [redacted] described the environment in the work unit supervised by [redacted]s very negatively and believed it was totally unacceptable. She also opined that [redacted]ri and [redacted] had a lengthy affair (Tab 6, Ex. D, Statement of [redacted]p. 1-3, paragraphs 2,3, 8, 9, 10-15; Ex. E, Memorandum from [redacted], dated 6 August 2008, pp. 1-3, paragraphs 3-6, 8-11, 13-14).

(2) [redacted]s also assessed [redacted] management and conduct as substandard (Tab 6, Ex. G, Memorandum of [redacted]s, p. 2, paragraph 2c; p. 3, paragraph 4).

(3) At [redacted] direction, [redacted] had begun and partially completed an internal ATSC investigation into [redacted] discovery of inappropriate material on [redacted] computer files (Tab 6, Ex. G, Memorandum of [redacted], p. p. 1, paragraph 1; p. 4, paragraph 5; Ex. H, Memorandum of [redacted] to COL Halstead, p. 1).

(4) The Fort Eustis Directorate of Information Management (DOIM) strictly adheres to the provisions of AR 25-1 and AR 25-2. The DOIM also monitors all government systems for improper use and employs appropriate safeguards. However, it did not discern any improper computer use by [redacted] (Tab 6, Ex. O, Statement of [redacted] p. 1; Ex. P, Statement of [redacted]tt, p. 1).

(5) [redacted] scored a 92% on her annual information technology assurance examination in January 2008 (Tab 6, Ex. W, Fort Eustis DOIM exam record).

## CONCLUSIONS

1. OSC Allegation 1. The allegation that Federal employees and contractors have sent e-mails containing sexually explicit photographs and jokes, and conversations of an obscene nature from government e-mail accounts during duty hours is substantiated. The specifics are described below.

(a) The allegation that [redacted] and [redacted] have sent e-mails from government e-mail accounts containing explicit pornographic or sexually explicit images is substantiated. E-mails between the two confirm [redacted] sent more than one sexually explicit image to [redacted] and others, and that [redacted] forwarded sexually explicit photos to another Federal employee [redacted] and to a Soldier ([redacted] in 2005 and 2006, respectively.

(b) The allegation that [redacted], [redacted], [redacted], [redacted], [redacted] and [redacted] have sent e-mails from government e-mail accounts containing jokes and humor of a sexual nature, discussions of sexual encounters between employees, and other inappropriate material is substantiated. E-mail messages authored and/or exchanged among all of the persons named above are contained in an exhibit attached to the investigation. Further, although [redacted] admits to receiving but not forwarding inappropriate e-mail, that exhibit does contain an e-mail he authored which is extremely suggestive in that it hints strongly at one or more clandestine rendezvous for sexual purposes with [redacted]. There are also photos of [redacted] in various states of dress on the hard drive of [redacted] old computer.

2. OSC Allegation 2. The allegation that [redacted] used Federal employees [redacted] and [redacted]' access cards and computer passwords between October 2007 and January 2008 is substantiated. Witnesses conclusively state they observed [redacted] using CACs of others and accessing their computers. [redacted] admitted this was likely. Although [redacted] and [redacted] both asserted this was done in furtherance of mission completion, the former's actions were at least technical violations of AR 25-2.

## CORRECTIVE ACTIONS

1. Disciplinary action was proposed to suspend [redacted] from her duties at the ATSC, Fort Eustis, for a period of five days for misuse of government property and resources, and for conduct unbecoming a federal employee (Addendum, enclosure 2). This is consistent with the recommendation of the AR 15-6 investigating officer regarding [redacted] Her grade, apparent remorsefulness, and treatment of similar offenses in the past were considered in proposing this action. The action was initiated and proposed by the Headquarters, TRADOC, Deputy Chief of Staff, G-3/5/7 level to preclude any perceptions of bias by persons at ATSC. Subsequent to her receipt of the proposal memorandum, [redacted] retired from Federal service on 31 October 2008.

2. Disciplinary action in the form of a written counseling statement has been issued to [redacted] for his failure to provide effective and appropriate leadership, and to exercise sound judgment, when the issues involved in this matter were initially presented to him

(Addendum, enclosure 3). This is also consistent with the recommendation of the AR 15-6 investigating officer. The facts that [redacted] did take action to investigate by referring the matter to CID, and investigated further by reviewing TDY vouchers to ascertain whether [redacted]'s official travel coincided with [redacted] has been considered. The action was taken by [redacted]'s supervisor, the TRADOC Assistant Deputy Chief of Staff, G-3.

3. Evidence gathered was referred to the second-level supervisor of [redacted] within the TRADOC Deputy Chief of Staff, G-3/5/7, [redacted], for his misuse of government property in transmitting an inappropriate e-mail message to [redacted] during duty hours. While he apparently did not transmit other inappropriate e-mail and images on his computer, and the e-mail at issue is several years old, his grade (GS-13) and lack of total candor to the investigating officer merited counseling. [redacted] as issued a written counseling to [redacted] (Addendum, enclosure 4).[16]

4. TRADOC Deputy Chief of Staff, G-3/5/7 leaders have directed appropriate professional training from the Equal Employment Opportunity (EEO) staff and others to ensure that ATSC leadership and workforce are aware of and prepared to act on EEO-related matters as well as other sensitive management issues in the workplace.

5. TRADOC Deputy Chief of Staff, G-3/5/7 leaders have also directed a review of the ATSC supervisory structure and rating schemes to help ensure all employees and managers are rated by appropriate supervisors, and that those supervisors are aware of their supervisory responsibilities.

6. Collateral Issues.

a. Federal contractor employees are employed by the contractor performing a government contract and are obviously not Federal employees. Both [redacted] and [redacted] are Federal contractor employees and have committed misconduct in the government workplace. [redacted] exchanged many inappropriate and more than one sexually explicit e-mail messages and attachments to [redacted] during duty hours. Further, regardless of whether he used his personal computer to do so, he clearly used his AKO account to transmit the e-mail. Although [redacted] stated he does not recall receiving sexually explicit e-mail from [redacted] he exchanged a number of sexually suggestive e-mails with her during duty hours. The results of this investigation were referred to the Adjutant General, State of Pennsylvania, Joint Forces Headquarters, Fort Indiantown Gap, Pennsylvania, to ensure Coalescent Technology, [redacted] current employer, is aware of his misconduct and consideration is given to appropriate actions under the Coalescent Technology contract. The Adjutant General replied that [redacted] contract expires in November 2008 and will not be renewed. Further, the results of the AR 15-6 investigation were referred to his supervisor at Coalescent Technology for appropriate action (Addendum, enclosure 5). The results of this investigation were also

[16] The IO also considered an allegation by [redacted] that she "believed" [redacted] had received a government laptop for her use by [redacted]. He did not pursue this action further because of a lack of specifics and direct relevance to his investigation.

provided to legal counsel to the contracting officer at ATSC to ensure [redacted] employer, Wire One, is aware of his misconduct and consideration is given to appropriate actions under the Wire One contract. Legal counsel determined that the misconduct occurred under a now-expired contract and ATSC was without a contractual remedy against [redacted] his employer. However, legal counsel will address [redacted] conduct with the contractor to ensure that the proper use of government equipment and e-mail usage is communicated to all employees and subcontractor employees (Addendum, enclosure 6). Finally, AKO administrators will be notified of this misuse of government computers and the AKO system so that they may initiate action they deem appropriate concerning the contractor employees.

b. [redacted], [redacted] hy, and [redacted] are retired from government service. [redacted] clearly engaged in misconduct and mismanagement while employed at ATSC. [redacted] alleged to have committed misconduct, and [redacted] is alleged to have been, at the least, negligent in performing her supervisory duties and responsibilities. However, as all are no longer Federal employees, they cannot be disciplined for their conduct.

c. [redacted] the AR 15-6 IO, determined that there were no systemic problems with the procedures and systems that educated employees and enforce compliance AR 25-1 and 25-2. Rather, he opined that management lapses facilitated the misconduct and attributed much of it [redacted]s' failure to exercise good management practices. As noted above, [redacted] is now retired and not subject to discipline or corrective action.

d. Results of the investigation revealed that the employees discussed in the paragraphs above most probably engaged in sexual liaisons facilitated by their misuse of government computer systems and e-mail. One witness, [redacted] alleged she was sent home early (at 3 or 4 PM) on occasion so that [redacted] and [redacted] could spend time together. However, there is no evidence that [redacted] and [redacted] or any of the other subject employees, engaged in this conduct during duty hours or at the duty site.

e. There were no criminal violations evident; therefore, all actions taken against persons responsible were administrative.

## CLOSING COMMENTS

Federal employees must conduct themselves in a professional manner and refrain from using government resources and time for their own benefit. Further, they must not engage in conduct that tends to disgrace, discredit, or is in any way prejudicial to the Federal service in the conduct of its service to our nation.

The Army takes its responsibility to address concerns brought to it by the OSC very seriously. The Army has addressed the concerns raised in the instant allegations

deliberately and thoughtfully. The planned corrective actions are intended to hold the responsible persons accountable and deter future, similar misconduct. Further, the additional training and reviews cited should help to ensure all employees are aware of their individual responsibilities and the Army's expectations for them.

This letter, with enclosures, is submitted in satisfaction of my responsibilities under Title 5, USC, Sections 1213 (c) and (d).

Sincerely,

21 Nov 08

Assistant Secretary of the Army
(Manpower & Reserve Affairs)

DECLARATION

Pursuant to 28 U.S.C. Section 1746, I, [redacted] make the following declaration.

1. I possess a Ph.D. in Systems and Information Engineering from the University of Virginia, and I have significant contributions in the field within peer-reviewed publications. I consider myself a data mining expert.

2. On 4 August 2008 I was appointed as an AR 15-6 Investigating Officer to investigate misconduct by Federal employees and contractor employees at Army Training Support Center (ATSC), Fort Eustis, Virginia. I completed my investigation on or about 14 August 2008.

3. During the course of my investigation, I reviewed [redacted] current (as of August 2008) e-mail folders and found previously undiscovered additional images and movies that were sexually explicit and inappropriate (included on discs in my investigation). I am aware [redacted] and [redacted] ATSC employees who reviewed the contents of [redacted] computer in May 2008, did not discover that material. I conclude that they did not find everything I found because the additional material was added after they reviewed the e-mail folders in May, or because my advanced academic training enabled me to discover that material.

I declare under penalty of perjury that the foregoing is true and correct. Executed on November 7, 2008.

[redacted]
Colonel, U.S. Army

# 1

DEPARTMENT OF THE ARMY
HEADQUARTERS UNITED STATES ARMY TRAINING AND DOCTRINE COMMAND
102 MCNAIR DRIVE
FORT MONROE VIRGINIA 23651-1047

REPLY TO
ATTENTION OF

ATJA

14 August 2008

MEMORANDUM FOR MG Abraham J. Turner, Deputy Chief of Staff, G-3/5/7, HQ TRADOC, Fort Monroe, VA 23651

SUBJECT: Findings and Recommendations of Investigating Officer

I. Background

On or about 30 April 2008, [redacted] (b)(6) (contractor employee for Support Directorate) conducted a life cycle replacement of [redacted] (b)(6) (Federal employee) former computer in building 1514 on Fort Eustis, Virginia (Exhibits A and B). In accordance with the Army Training Support Center's information technology procedures, [redacted] (b)(6) asked the supervisor, [redacted] (Federal employee), if she required any of the replaced computer's data. Concerned with maintaining historical knowledge of the Video Tele-Training and the Satellite Education Network programs, [redacted] requested [redacted] (b)(6) to transfer the hard drive's data to the shared portal. [redacted] (b)(6) had difficulty transferring the hard drive data. He, therefore, physically removed the hard drive and gave the hard drive to [redacted] for safekeeping.

In addition, [redacted] attempted to obtain the historical files by coordinating with [redacted] (b)(6) [redacted] (b)(6) new supervisors, [redacted] (b)(6) (retired Federal employee) and [redacted] (b)(6) (Federal employee) (Exhibit B). When [redacted] (b)(6) transferred her position from the Video Tele-Training program to TSSD Operations [redacted] (b)(6) "re-ghosted" [redacted] (b)(6) new computer within TSSD Operations and transferred her former Video Tele-Training and Satellite Education Network files to her new computer on or about 12 February 2008 (Exhibit A). The "ghost" image is Army Training Support Center's baseline information technology configuration. As of 13 May 2008, [redacted] had not received all of the historical files obtained through coordination. [redacted] (b)(6) had not transferred the Satellite Education Network files (Exhibit B).

On or about 14 May 2008, [redacted] took her government laptop computer and the removed hard drive to her off post residence to continue working from home (Exhibits B and N). [redacted] (b)(6) (Federal employee) assisted [redacted] with connecting the removed hard drive to the government laptop. Able to read the removed hard drive, [redacted] began searching and downloading relevant Video Tele-Training and Satellite Education Network files. During her search, [redacted] discovered pornographic and other inappropriate images and PowerPoint presentations within email folders [redacted] (b)(6) had emailed some of these

images and PowerPoint presentations to Soldiers, Federal employees, and Federal contractors. [redacted] consolidated her findings (Exhibit F) and provided them to [redacted] (Federal employee and Deputy Director of Army Training Support Center) on or about 19 May 2008 (Exhibits B and G).

[redacted] delivered the images and PowerPoint presentations contained in [redacted] email to the Acting Executive Director, [redacted] (Federal employee). [redacted] consulted Army Criminal Investigation Division and his Support Directorate (Exhibits K and L). At the advice of these technical staffs, [redacted] instructed Support Directorate to seize the removed hard drive, [redacted] computer, [redacted] (retired Federal employee) old computer, and [redacted] new computer (Exhibits B, G, K, and L). Army Criminal Investigation Division informed [redacted] that [redacted] iscovery may have been improper (Exhibit K).

At 11:00AM on 27 May 2008, [redacted] hosted a leadership meeting with [redacted] and [redacted] s (Exhibits B, G, I, J, and K). The Deputy Director, [redacted] was not present. [redacted] understood the purpose of the meeting was to discuss how to proceed with Ms. Ahrens' discovery (Exhibits B, I, and J). Rather than address the discovered images and the organization's appropriate response, [redacted] focused the discussion on other items. [redacted] focused on a single email thread between [redacted] and himself. [redacted] additionally focused on [redacted] method of discovery (Exhibits B, I, and J). Lastly, [redacted] read [redacted] the civilian table of punishment and penalties, directing the statements at [redacted] (Exhibits B and I). The meeting never discussed [redacted] images and PowerPoint email files (Exhibits B, I, and J).

Unknown to [redacted] at this time, [redacted] directed [redacted] to continue the investigation of [redacted] Army Regulations 25-1 and 25-2 violations (Exhibits G, H, and K). [redacted] is currently investigating the violations (Exhibit H).

Without knowledge that [redacted] had directed [redacted] to investigate the alleged violations by [redacted] [redacted] s solicited the help of her [redacted] (Federal employee) to use Mr. Seger's (Senior Executive Service, TRADOC Deputy G3) open door policy (Exhibits B, M, and N). [redacted] organization, the Army Training Support Center, is a Field Operating Agency under the direction of the TRADOC G3. [redacted] works within the TRADOC G3 and his office is within close proximity to Mr. Seger's office. Without physical evidence, [redacted] represented his [redacted] complaint to [redacted] (Mr. Seger's Deputy and Federal employee) (Exhibits B, M, and N). [redacted] obtained legal counsel from [redacted] of the TRADOC Staff Judge Advocate's office. On that counsel, [redacted] informed Mr. Seger of the situation and preserved Mr. Seger's potential decision authority over this allegation by only discussing generalities. [redacted]

(b)(6) called [redacted]s and offered her an office call to obtain physical evidence and firsthand knowledge (Exhibit B). [redacted] declined (b)(6) offer (Exhibit B). (b)(6) under Mr. Seger's guidance, informed (b)(6) not to discuss the allegations since the issue was not within his chain of command. (b)(6) also stated that [redacted] could use Mr. Seger's open door policy, but advised against it repeating that [redacted] would potentially require Mr. Seger as a decision authority concerning the allegations.

On 4 August 2008, Major General Abraham Turner (Deputy Chief of Staff, TRADOC G3/5/7) appointed (b)(6) as an Army Regulation 15-6 Investigating Officer responsible for investigating the allegations forwarded by the Office of Special Counsel, Merit Systems Protection Board.

II. Investigation

On 4 August 2008, I, (b)(6), began the investigation by consulting the designated legal advisor, (b)(6) In the course of the investigation, I personally interviewed seventeen people connected with the allegations, beginning with (b)(6) and ending with (b)(6) I obtained thirteen sworn statements, four official memorandums of record, one certified email statement, and records of conversations with (b)(6) (b)(6) In the course of the investigation, I have determined the following facts:

a. [redacted] obtained (b)(6) former hard drive as a result of the Army Training Support Center Support Directorate's legitimate standard operating procedures concerning life cycle replacement, computer imaging, and data transfer (Exhibit A, B, and G). The TRADOC Staff Judge Advocate's office interpretation of Army Regulation 25-2, Chapter 4, paragraph 4-5a(7) permits [redacted] search of information on (b)(6) government hard drive while executing her supervisory responsibilities. Further, because [redacted] government laptop frequently travels with her, connecting the hard drive to the government laptop did not violate Army Regulation 25-2, Chapter 4, paragraph 4.5a(5). (b)(6) investigation concurs with these legal interpretations (Exhibits G and K).

b. [redacted] discovered sexually explicit material and other inappropriate material attached to (b)(6) outgoing email in the form of images and PowerPoint presentations (Exhibits B and F). Examples include inappropriate images of (b)(6) (b)(6) (Federal employee of TRADOC G3/5/7) in undergarments; sexually explicit material attached to email sent to (b)(6) dated 12 September 2006; sexually explicit material attached to email sent to (b)(6) (b)(6) dated 5 June 2006; sexually explicit material attached to email sent to (b)(6) dated 2 June 2006; inappropriate image attached to email sent to (b)(6) dated 9

March 2006; sexually explicit material in a PowerPoint presentation attached to email sen (b)(6) dated 9 December 2005; and inappropriate email images attached to email sent to numerous recipients, dated 2 November 2005 (Exhibit F).

c. [redacted] discovered sexually explicit material attached to (b)(6) incoming email from (b)(6) dated 9 December 2005, 2 June 2006, and 5 June 2006 (Exhibit F). (b)(6) used his AKO account and it can not be determined whether he used a government computer or a personal computer. (b)(6) states that he uses three computers simultaneously while working, with at least one personal computer within the suite (Exhibit T).

d. [redacted] and (b)(6) (Federal employee) observed (b)(6) using (b)(6) CAC card and email numerous times (Exhibits B, and D). [redacted] (b)(6) and (b)(6) (Federal employee) observed (b)(6) using (b)(6) CAC card and email (Exhibits B, C, and D). (b)(6) believes (b)(6) (b)(6) use of (b)(6) CAC card promoted the government's interest by facilitating mission accomplishment (Exhibit C). (b)(6) indicates she may have used (b)(6) CAC cards and email, but only for her understanding of official government uses (Exhibit V).

e. (b)(6) describes (b)(6) work environment as inconsistent with the standards of Army Regulation 600-20, Chapter 7, paragraph 7-4a(3) (Exhibits D and E). (b)(6) describes (b)(6) work environment in a similar manner (Exhibit G).

f. (b)(6), Deputy Director of Army Training Support Center, is conducting an informal investigation of (b)(6) alleged violations of Army Regulations 25-1 and 25-2. At the time of this report, he has not made a determination (Exhibit G and H).

g. (b)(6) leadership meeting on 27 May 2008 failed to address the organization's response to (b)(6) possible misuse of government equipment to transmit sexually explicit material and other inappropriate material. (b)(6) and (b)(6) describe (b)(6) focusing on one email thread between (b)(6) focusing on [redacted] ethod of discovering the sexually explicit material and other inappropriate images (Exhibits B, I, and J). (b)(6) substantiates [redacted] statement that (b)(6) directed the Civilian Table of Punishment and Penalties at [redacted] (Exhibits B and I). (b)(6) felt (b)(6) was trying to cover up something by focusing on the single email thread, rebuking [redacted] discovery, and not addressing the issue (Exhibit J). (b)(6) further

summarizes the meeting by stating that he had never in the lifetime of his career observed a senior leader act like (b)(6) In the (b)(6) opinion, (b)(6) (b)(6) does not understand command responsibilities and failed to focus on the relevant facts, which concerned (b)(6) (Exhibit J).

h. (b)(6) acknowledges addressing two alleged Army Regulation 25-1 and 25-2 violations. He is investigating sexually explicit material found on (b)(6) computer. He also stated that [redacted] printing of the material was "irregular." (b)(6) focus on [redacted] stems from the Army Criminal Investigation Division's statement to (b)(6) that [redacted] actions may have been improper (Exhibit K).

i. (b)(6) (Federal employee) did not find additional sexually explicit material on (b)(6) computer (Exhibit L). (b)(6) did find "inappropriate" images attached to email sent from (b)(6) government computer to other email recipients (Exhibit L). He did not discover sexually explicit material or other inappropriate images on (b)(6) old and new computers and [redacted] computer (Exhibit L).

j. (b)(6) informed (b)(6) of Mr. Seger's open door policy and the implications associated with using the policy (Exhibits M and N). (b)(6) further encouraged [redacted]s to discuss the situation with him and [redacted] declined (Exhibit B).

k. Fort Eustis DOIM strictly adheres to the Army Regulations 25-2 and 25-2. Further, the DOIM monitors all government systems for improper use utilizing the SMS system. The Fort Eustis DOIM never discovered [redacted] improper use of government systems (Exhibits O and P).

l. (b)(6) did not recall receiving sexually explicit email from (b)(6) (Exhibit Q). (b)(6) further stated that he deletes and does not forward "inappropriate" email he receives (Exhibit Q).

m. (b)(6) acknowledges receiving "adult explicit material" from (b)(6) in the past (Exhibit R). (b)(6) also states he does not forward this material, but does delete it (Exhibit R).

n. (b)(6) refused to provide an official statement (Exhibit S). However, he did wish to express that (b)(6) is a loyal government employee. He found the allegations "hard to comprehend." He also shared that (b)(6) was a "church-

going" woman and "loving grandmother" (Exhibit S).

o. [redacted] physically works at Fort Indiantown Gap, Pennsylvania and no longer works for Alion Science and Technology. He declined to provide his contract supervisor contact information. His current federal contract through Coalescent Technology provides service to the Army National Guard Bureau. [redacted] remains in email contact with [redacted]. [redacted] states that he does send [redacted] "adult content" email, but personally does not classify such email as pornographic. [redacted] also informed me that he uses three computers at work, with at least one personal computer within the suite. He further stated that he never used government computers to send "adult content" material to [redacted] (Exhibit T).

p. [redacted] was never a government employee with TRADOC. Personnel and security checks validated that [redacted] was never a member of the armed services, a Department of the Army civilian employee, or a federal contractor (Exhibit U).

q. [redacted] admits that she used [redacted] CAC cards while both were present. She states that the CAC card use occurred with government business. She also states that she may have used [redacted] computer to send email when [redacted] was not present. She also admits that she has personal photographs on her computer. She is remorseful for her choices (Exhibit V).

r. [redacted] scored a 92% on her annual information technology assurance examination (Exhibit W).

s. [redacted] (Investigating Officer) found additional sexually explicit images and movies within [redacted] email folders, mostly contained within her sent and deleted folders. These images include personal sexually explicit images. The inspection also discovered all the images and PowerPoint presentations found by [redacted] These images are consolidated on a compact disc, labeled '[redacted] Images 12 Aug 08" (Exhibit X). In the inspection, legitimate government work dominated the files. The sexually explicit images were sporadic.

t. [redacted] obtained the images from [redacted] saved email files, which are consolidated within five compact discs (Exhibit Y).

III. Findings

a. [redacted] improperly used government equipment to transmit sexually explicit and other inappropriate material. Examples include inappropriate images of

[redacted] in undergarments; sexually explicit material attached to email sent to [redacted] dated 12 September 2006; sexually explicit material attached to email sent to [redacted] dated 5 June 2006; sexually explicit material attached to email sent to [redacted], dated 2 June 2006; inappropriate image attached to email sent to [redacted] r. [redacted], dated 9 March 2006; sexually explicit material in a PowerPoint presentation attached to email sent [redacted] dated 9 December 2005; and inappropriate email images attached to email sent to numerous recipients, dated 2 November 2005 (Exhibit F). [redacted] may have used government equipment to transmit sexually explicit material. [redacted] used his AKO account and it can not be determined whether he used a government computer or a personal computer. [redacted] states that he uses three computers simultaneously while working, with at least one personal computer within the suite (Exhibit T). Both are violations of Army Regulation 25-1, Chapter 6, paragraph 6-1f(1) and Army Regulation 25-2, Chapter 4, paragraph 4-5r(7). No evidence exists suggesting that [redacted] transmitted sexually explicit or inappropriate material (Exhibits L, Q, R, and S). No federal employment records exist for [redacted] serving as a member of the armed forces, a federal employee, or a federal contractor (Exhibit U).

b. [redacted] improperly shared CAC cards and passwords, violating Army Regulation 25-2, Chapter 4, paragraph 4-5a(8) (Exhibits B, C, D, and V). [redacted] improperly accessed [redacted] email accounts, violating Army Regulation 25-2, Chapter 4, paragraph 4-5s(9) (Exhibits B, C, D, and V). No evidence exists suggesting the others improperly shared passwords and accessed other user email accounts.

c. No systemic shortfalls allowed for the misconduct. Both the Fort Eustis DOIM and the Army Training Support Center's information technology staff (Support Directorate) strictly adhere to Army Regulations 25-1 and 25-2 (Exhibits A, L, O, and P). Both also create and execute procedures and systems that enforce employee compliance of these regulations. However, management shortfalls enabled the misconduct. [redacted] created a work environment that permitted the misconduct by not enforcing Army Regulations 25-1 and 25-2 (Exhibits B, D, E, and H).

d. [redacted], former Chief of Video Tele-Training, and [redacted] previous supervisor, tolerated an environment that permitted inappropriate conduct and contributed to the current environment within the Video Tele-Training (Exhibits B, D, E, and H). [redacted] (Executive Director of Army Training Support Center)

did not provide effective leadership in addressing these issues when brought to his attention. When initially addressing the alleged violations of Army Regulations 25-1 and 25-2, (b)(6) focused on perceived violations by the reporting individual, partially due to incorrect advice he received from technical staff. However, his initial focus on the reporting individual and lack of attention to the underlying violations reported created the perception that management tolerated the inappropriate conduct and would not effectively deal with complaints concerning that conduct (Exhibits B, I, J, and K). This created the perception among some employees that management approved of the inappropriate conduct and would resent efforts to correct it.

IV. Recommendations

a. (b)(6) supervisors take appropriate remedial and disciplinary action against her for her violations of AR 25-1 and AR 25-2.

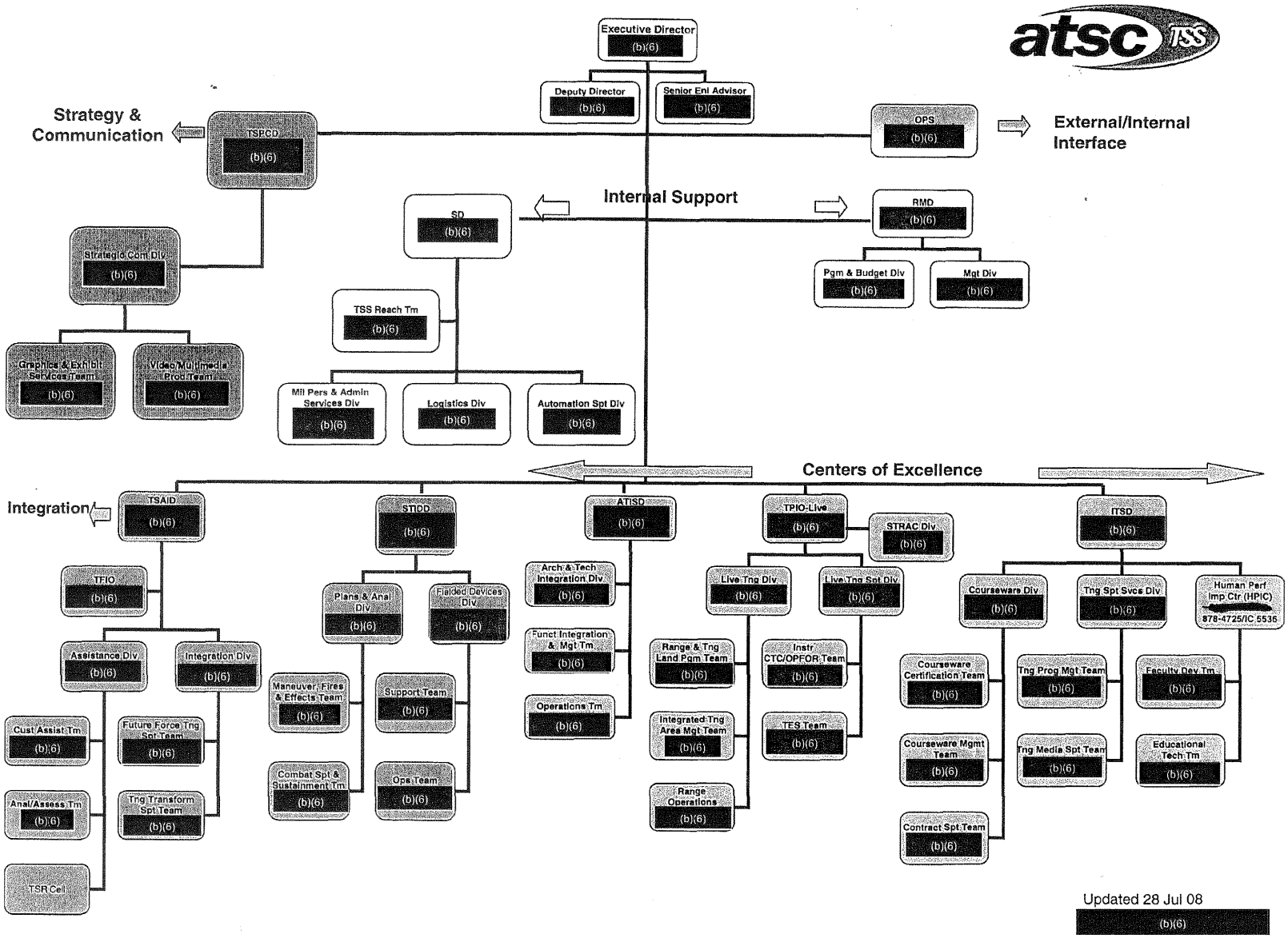
b. (b)(6) supervisors take appropriate remedial and disciplinary action to address his failure to exercise appropriate leadership and use sound judgment in his attempts to resolve the issues identified in this investigation when they were made known to him in May 2008.

c. ATSC leaders receive appropriate professional training designed to enhance their ability to effectively lead their organization and to appropriately respond to Equal Employment Opportunity issues.

d. Headquarters, TRADOC, Deputy Chief of Staff, G-3/5/7 leaders review the ATSC supervisory structure and rating schemes to ensure all employees and managers are supervised and rated appropriately and fairly.

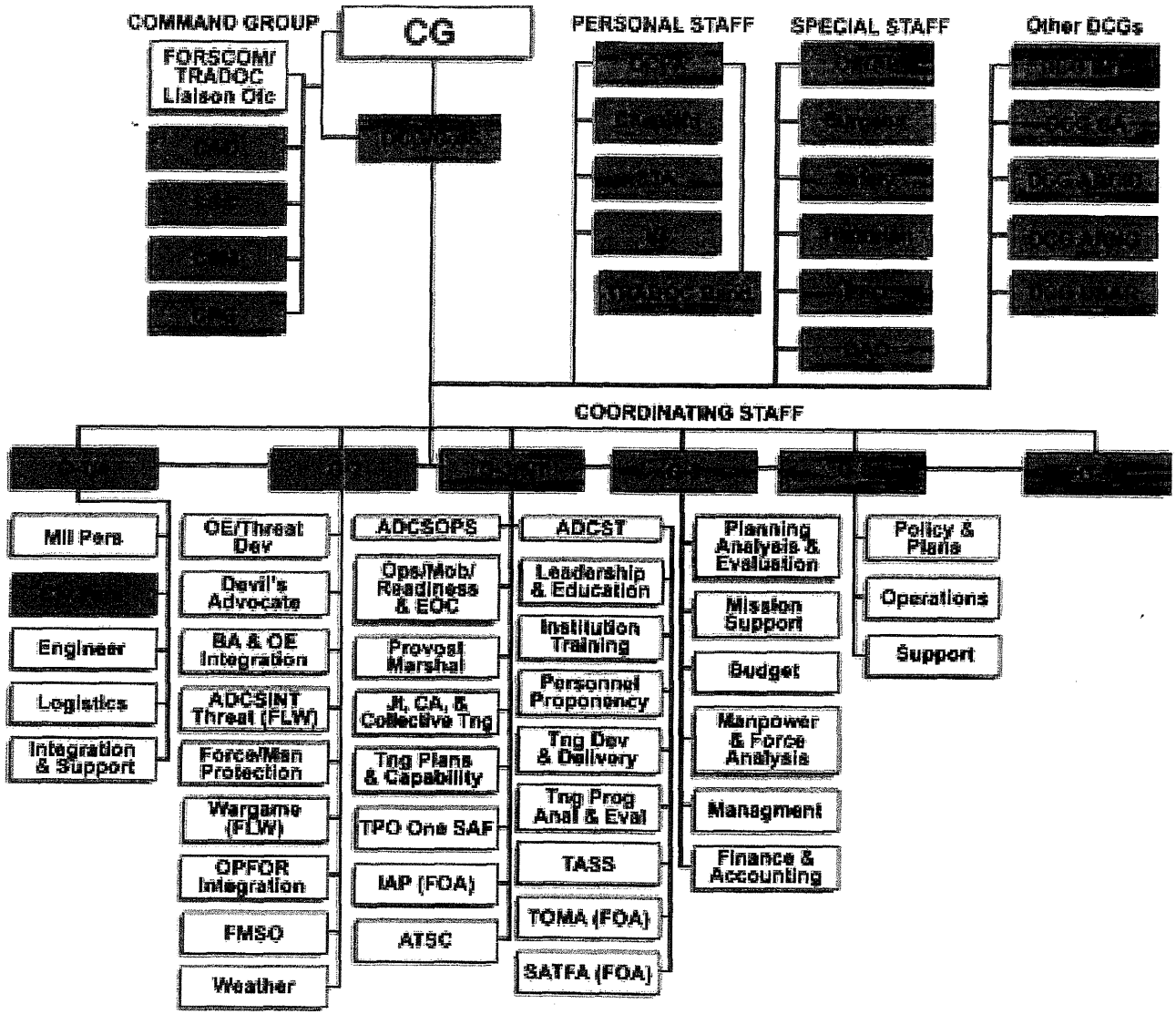
(b)(6)
Investigating Officer

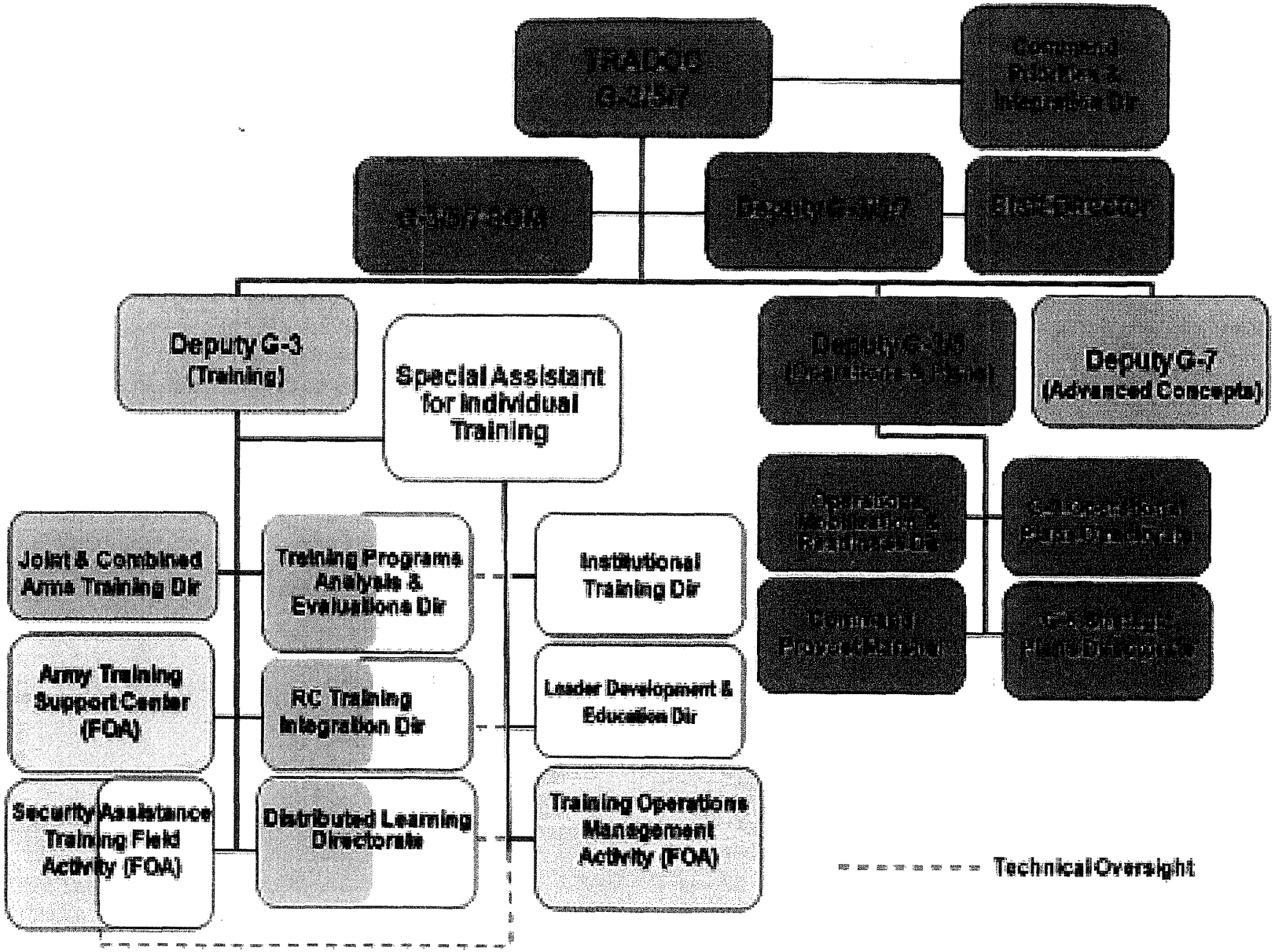
# 2




Updated 28 Jul 08

(b)(6)


COMMAND GROUP
CG
FORSCOM/ TRADOC Liaison Ofc
PERSONAL STAFF
SPECIAL STAFF
Other DCGs
COORDINATING STAFF
Mil Pers
Engineer
Logistics
Integration & Support
OE/Threat Dev
Devil's Advocate
BA & OE Integration
ADCSINT Threat (FLW)
Force/Man Protection
Wargame (FLW)
OPFOR Integration
FMSO
Weather
ADCSOPS
Ops/Mob/ Readiness & EOC
Provost Marshal
Jt, CA, & Collective Trng
Trng Plans & Capability
TPO One SAF
IAP (FOA)
ATSC
ADCST
Leadership & Education
Institution Training
Personnel Proponency
Trng Dev & Delivery
Trng Prog Anal & Eval
TASS
TOMA (FOA)
SATFA (FOA)
Planning Analysis & Evaluation
Mission Support
Budget
Manpower & Force Analysis
Managment
Finance & Accounting
Policy & Plans
Operations
Support


TRADOC G-2/5/7
Command Priorities & Integration Dir
Deputy G-3 (Training)
Special Assistant for Individual Training
Deputy G-7 (Advanced Concepts)
Joint & Combined Arms Training Dir
Training Programs Analysis & Evaluations Dir
Institutional Training Dir
Army Training Support Center (FOA)
RC Training Integration Dir
Leader Development & Education Dir
Security Assistance Training Field Activity (FOA)
Distributed Learning Directorate
Training Operations Management Activity (FOA)
Technical Oversight