governmentattic.org
"Rummaging in the government's attic"

Description of document:	Army Criminal Investigation Command (CID) Annual Historical Review 2013-2014, 2015
Requested date:	13-July-2016
Released date:	15-September-2016
Posted date:	31-October-2016
Source of document:	FOIA Request U.S. Army Criminal Investigation Command Crime Records Center ATTN: CICR-FP Russell Knox Building 27130 Telegraph Road Quantico, VA 22134-2253

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.

-- Web site design Copyright 2007 governmentattic.org --

DEPARTMENT OF THE ARMY
U.S. ARMY CRIMINAL INVESTIGATION COMMAND
U.S. ARMY CRIME RECORDS CENTER
27130 TELEGRAPH ROAD
QUANTICO, VA 22134

REPLY TO
ATTENTION OF

SEP 15 2016

FA16-3483

This is in further response to your request for release of information from the files of the U.S. Army Criminal Investigation Command (USACIDC) and supplements our response of August 3, 2016. Your initial request was received on July 13, 2016.

The enclosed U.S. Army Criminal Investigation Command Annual Historical Review 2013-2014, responsive to your request, is part of a system of records exempt from the disclosure provisions of the Freedom of Information Act (FOIA). The names of law enforcement personnel, as well as names, social security numbers and other personal items of information pertaining to third parties have been withheld. The removal of this information constitutes a partial denial pursuant to Title 5, USC, Section 552, Exemptions (b)(6), and (b)(7)(C) of the FOIA, because release could violate the personal privacy of other individuals mentioned in the report.

This partial denial, which is made on behalf of Major General Mark S. Inch, Commander, USACIDC, the Initial Denial Authority for USACIDC records under the FOIA, may be appealed to the Secretary of the Army.

If you decide to appeal at this time, your appeal must be submitted within 90 days of the date of this letter. In your appeal, you must state the basis for your disagreement with the partial denial and you should state the justification for its release. Your appeal is made through this Center and should be addressed to the Director, U.S. Army Crime Records Center, (FA16-3483) 27130 Telegraph Road, Quantico, Virginia 22134, for forwarding, as appropriate, to the Office of the Secretary of the Army, the appellate authority. Please note that your appeal should address information denied in this response and cannot be used to make a new request for additional or new information.

Questions regarding this action should be addressed in writing to the address shown on the letterhead or by calling 571-305-4231. Please reference the above control number on any correspondence.

Sincerely,

Susan Cugler
Director, Crime Records Center

Submitted by:
The Gemini 3 Group, Inc.
292 Garrisonville Road
Suite 201
Stafford, VA 22554

UNITED STATES ARMY CRIMINAL INVESTIGATION COMMAND ANNUAL HISTORICAL REVIEW 2013-2014

★ ★ ★ ★ ★ ★ ★ ★ ★

United States Army Criminal Investigation Command

Annual Historical Review 2013-2014

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

Gemini 3 Group, Inc.

Acknowledgements

The author would like to thank Dr. (b) (6), (b) (7)(C) for his guidance and advice during the many stages of interviewing, researching, writing, and editing. Thank you to Dr. (b) (6), (b) (7)(C) for his initial support of the project.

I would also like to thank (b) (6), (b) (7)(C) and the entire Gemini 3 Group for their support throughout the past year.

Many thanks to (b) (6), (b) (7)(C) and the CID Public Affairs Office for their assistance in providing resources, arranging interviews, and much more.

Thank you to MG (b) (6), (b) (7)(C) and all the CID personnel who took the time to interview with my colleagues and I, providing excellent information and insight that allowed the report to truly tell your story.

Thank you to all members of CID for your invaluable service to our country.

Preface

The United States Army Criminal Investigation Command (USACIDC) traces its lineage to the Criminal Investigation Division (CID) established in 1918 at the direction of General John J. Pershing. The division provided a greater investigative capability to the newly formed Military Police Corps as they oversaw the American Expeditionary Forces during World War I.

The unit evolved over the decades, ultimately being established as the United States Army Criminal Investigation Command on September 17, 1971. Though no longer a division, now with command authority and jurisdiction over the entire Army, the command is still largely called CID today. The command has continued to evolve, becoming an integral part of the Army under the Provost Marshal General. Responsible for all felony investigations involving the Army or its personnel, CID has a global mission and pursues many kinds of crimes, which will be analyzed in the following report.

This Annual Historical Review was contracted to the Gemini 3 Group, Inc. in July 2014, with the scope of the report encompassing calendar years 2013 and 2014. The research process included examining command documents, current manpower and financial data, and the command magazine, *The Shield*, from the past several years. In addition to this gathering of resources, the research team conducted a large number of interviews with current and former CID personnel. (b) (6), (b) (7)(C) was the primary interviewer and writer of the report, with interviewing and editorial assistance from Dr. (b) (6), (b) (7)(C). Dr. (b) (6), (b) (7)(C) provided preliminary project support.

(b) (6), (b) (7)(C)
May 2015

The Author

(b) (6), (b) (7)(C) graduated from the University of Mary Washington in 2014 with a Bachelor of Arts in History, with an emphasis in Military History. He graduated With Highest Distinction (Summa Cum Laude), completing his degree in only two years. During that time he was also a visiting student at the School of History, Classics, and Archaeology at the University of Edinburgh, Scotland.

Table of Contents

Chapter 1: Organization & Structure	1
Chapter 2: Policy & Procedure	12
Chapter 3: Manpower & Resources	31
Chapter 4: Operations	53
Chapter 5: Outreach	78
Chapter 6: Forging the Future	98
Glossary	104
Bibliography	117

List of Figures

Fig. 1: CID Command Structure	11
Fig. 2: CID Total Authorizations by Unit, FY12, FY13, & FY14	32
Fig. 3: CID Reserve Units	37
Fig. 4: CID National Guard Units	38
Fig. 5: CID Budget, FY13 & FY14	48
Fig. 6: CID Solve Rates in Percentages, FY13 & FY14	54
Fig. 7: MPFU Recoveries, 2013 & 2014	58
Fig. 8: FXD Caseload	66
Fig. 9: GFXC, FXTs, & ACME Forensic Testing, FY13 & FY14	68

Chapter 1: Organization & Structure

The United States Army Criminal Investigation Command (USACIDC, or more commonly CID) has undergone several organizational changes over the past two years. The command's top leadership lies with the Provost Marshal General (PMG), who is not only the Commanding General (CG) of CID, but the head Army Corrections Command (ACC) and General Officer for the Military Police Corps (MPs) on the Army Staff. For the majority of the reporting period, the position of Provost Marshal was held by Major General (MG) (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) who served as the CG of CID since September of 2011. A Military Police officer for thirty-four years, MG (b) (6), (b) (7)(C) has held numerous positions throughout the Army. Such positions include Deputy G-3 and Chief of Staff of the 18th Airborne Corps, Commandant of the Military Police School, Commander of Task Force 134, and command of the Maneuver Support Center based in Ft. Leonard Wood, MO. He was appointed Brigade Commander over Abu Ghraib Prison in 2004 following the torture scandal. MG (b) (6), (b) (7)(C) holds a Master's Degree in computer science and assisted in the development and implementation of the Global Control and Command System (GCCS).[1] One of MG (b) (6), (b) (7)(C) primary goals as Provost Marshal was to unify the Military Police Regiment and integrate CID, the MPs, and Army Corrections into a more cohesive organization. His strategies to do so will be discussed throughout the report.

The current PMG is MG (b) (6), (b) (7)(C), who assumed command on September 12, 2014. His previous positions include Deputy Provost Marshal for United Nations Operation Somalia II,

[1] GCCS is a combined system of software, hardware, and procedures to provide intelligence and situational awareness for military commanders. It is a collection of integrated programs which are used for a number of different purposes, from organizing joint operations between branches of the Armed Forces to coordinating multinational efforts. GCCS is operated by the Defense Information Systems Agency (DISA) under the Department of Defense. See "GCCS – Joint," Defense Information Systems Agency, http://www.disa.mil/services/command-and-control/gccs-j.

Mogadishu and for United States Forces Japan, Yokota Air Base, and Deputy in the Office of the Provost Marshal for Corrections. He has a long career in the corrections field, serving as Chief of the Corrections and Internment Branch, Operations, Readiness and Mobilization Directorate under the Office of the Provost Marshal (OPMG), and Commandant of the United States Disciplinary Barracks in Ft. Leavenworth, KS. [redacted] has also served in multiple posts abroad, including Director of Detainee Operations for Combined Security Transition Command-Afghanistan as part of Operation Enduring Freedom and Chief of Staff of Task Force 134 (Detainee Operations) when General [redacted] was the Commander. Like his predecessor, he also served as the Commandant of the United States Army Military Police School (USAMPS). His last post before assuming the position of PMG was as Commander of the Combined Joint Interagency Task Force 435 as part of Operation Enduring Freedom in Afghanistan. Originally holding the rank of Brigadier General upon assuming the position of Provost Marshal, MG [redacted] was promoted on October 10, 2014.[2]

The Provost Marshal, as the Commanding General of CID and ACC, usually resides at the Pentagon, while the rest of the command group operates out of the Russell-Knox Building (RKB) on Marine Corps Base Quantico. Originally housed at Ft. Belvoir, VA, CID relocated to Quantico—along with all other Military Criminal Investigative Organizations (MCIOs)—in April 2011.[3] In addition to the CG, the command group is made up of the Deputy Commander, Chief Command Warrant Officer, and Command Sergeant Major.

---

[2] Major General [redacted], USACIDC, interview with [redacted], Dr. [redacted], and Dr. [redacted], Crystal City, VA, September 26, 2014, 1-5, 23; [redacted], "CID Change of Command," *The Shield*, October 2014; [redacted], "CID Commanding General Promoted to Major General," *The Shield*, November 2014; "Commanding General," U.S. Army Criminal Investigation Command, http://www.cid.army.mil/commander.html.

[3] [redacted], "All In: CID settles into new HQ in Quantico," *The Shield*, June 2011.

The Deputy Commander (or Deputy Commanding Officer, DCO) assists the Commanding General in leading CID. As the CG is triple-hatted and has large responsibilities beyond CID, the DCO is tasked with the day-to-day running of the organization. They also coordinate with the Group and Battalion commanders, supporting and enabling them to complete their missions. The DCO is based out of Quantico while the Provost Marshal is based out of the Pentagon. The current Deputy Commander is Colonel (b) (6), (b) (7)(C) who assumed the position in August of 2014. His previous assignments include Commander of the 701st MP Group in Quantico and Commander of the 504th MP Battalion which deployed to Kandahar, Afghanistan. COL (b) (6), (b) (7)(C) has created a new steering group of principal CID staff to support the CG and aid in the framing of command decisions. COL (b) (6), (b) (7)(C) was preceded by COL (b) (6), (b) (7)(C), who had previously served as the 701st MP Group commander as well. During his time as DCO, COL [redacted] focused on sustainment and supporting the drawdown of combat operations overseas. He is currently serving as the Deputy Commander of the Defense Forensics & Biometrics Agency (DFBA).[4]

The Command Chief Warrant Officer (CCWO) is a senior commissioned CID agent who acts as a top advisor to the CG and is his representative to the rest of the command. Though the CCWO is primarily responsible for warrant officer matters, the position advises the CG on all troop matters, including personnel placement and disciplinary actions. A key change to the position was the decision by MG (b) (6), (b) (7)(C) that the CCWO should accompany the Commanding General at the Pentagon for the majority of the time. The current CCWO is CW5 (b) (6), (b) (7)(C) who assumed the position in October 2013. CW5 [redacted] has served as a combat support MP, a

[4] COL (b) (6), (b) (7)(C), USACIDC, interview with (b) (6), (b) (7)(C) and Dr. (b) (6), (b) (7)(C), Quantico, VA, October 15, 2014, 1-5; COL (b) (6), (b) (7)(C), U.S. Army, phone interview with (b) (6), (b) (7)(C) and Dr. (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) 1-8; "Surveillance Photos (4 of 9)," *The Shield*, September 2014.

Corrections officer, and as a CID agent in various capacities. With 24 years of service as an agent, he is one of the longest continuously serving CID agents still on active duty. Before assuming the position of CCWO, CW5 [redacted] was the Group Operations Officer for the 202nd MP Group, until it disbanded.[5] Prior to October 2013, the CCWO was CW5 (b) (6), (b) (7)(C), who retired after almost 30 years of service, over 20 of which were as a CID agent. The first female CCWO, CW5 [redacted] was also the first to hold the position with its current responsibilities, which were established by then Provost Marshal BG (b) (6), (b) (7)(C) in 2010. CW5 [redacted] still works in CID, now as the Chief of the Policy Branch and the Executive Secretary to the Defense Criminal Investigative Organizations Enterprise-Wide Working Group (DEW Group).[6]

Another important member of the command group is the Command Sergeant Major (CSM). As the highest ranking non-commissioned officer (NCO) of CID, the CSM acts as a bridge between the enlisted personnel and their commanders. Similarly to the CCWO, the CSM acts in both an advisory role to the Commanding General as well as representing the CG to the soldiers of CID. That area of responsibility includes a number of subjects, including recruiting, training, discipline, and morale. Command Sergeant Major (b) (6), (b) (7)(C) is the current CSM. He assumed the position in October 2013. Originally in the Veterinary Corps, he has served as Command Sergeant Major for the 6th MP Group (CID) and the 19th MP Battalion (CID) in Yongsan, Korea prior to assuming his current position.[7] He was preceded by CSM (b) (6), (b) (7)(C) who intended to retire after over 20 years of service in the Army and CID.

---

[5] CW5 (b) (6), (b) (7)(C), USACIDC, interview with (b) (6), (b) (7)(C), Quantico, VA, October 24, 2014, 1-4.

[6] CW5 (b) (6), (b) (7)(C) (ret.), USACIDC, interview with (b) (6), (b) (7)(C), Quantico, VA, September 30, 2014, 1-5.

[7] CSM (b) (6), (b) (7)(C), USACIDC, interview with (b) (6), (b) (7)(C) and Dr. (b) (6), (b) (7)(C), Quantico, VA, October 15, 2014, 1-2.

However, he was selected to be the Army enlisted liaison to the Department of Veteran Affairs. During his time as Command Sergeant Major, CSM [redacted] promoted recruitment and NCO professional development, as well as reviving the Soldier of the Year competition.[8]

The Russell-Knox Building is also the headquarters of the 701st Military Police Group (CID). This Group oversees many specialized units which carry out a number of missions at home and abroad, including protective services, financial and cyber-crime, and anti-terrorism efforts. Prior to assuming the position of DCO, COL [redacted] was the commander of the 701st. He was replaced in July 2014 by COL [redacted], former commander of the Protective Services Battalion and member of OPMG.[9]

The Protective Services Battalion (PSB) is one such specialized unit which provides personal security for major Department of Defense (DoD), Joint Chiefs of Staff, and Department of the Army (DA) personnel as they travel across the globe. Furthermore, when foreign officials of similar status visit the United States, the PSB also provides their protective details. During the 2013-2014 period, PSB completed over 400 missions on U.S. soil and overseas, including the sending of special agents to U.S. Central Command (CENTCOM) to provide security for high-level Combatant Commanders. They protected two former Secretaries of Defense and one former Chairman of the Joint Chiefs as well as conducted several visiting foreign counterpart missions. These missions took place in the greater Washington, D.C. area and throughout the country, for events such as the State of the Union Address. Additionally, PSB oversaw the

---

[redacted] "CID Salutes CSM [redacted]" *The Shield*, September 2013.

"701st MP Group (CID) Change of Command," *The Shield*, August 2014.

protective services for Combatant Commanders at U.S. Southern Command (SOUTHCOM) and U.S. Forces Korea (USFK).[10]

The Computer Crime Investigative Unit (CCIU) pursues and defends against "intrusions, related malicious activities, and insider criminal misuse of Army computers, networks, and data." The CCIU is an important part of the new Strategy for Operating in Cyberspace implemented by the DoD and actively supports the U.S. Army Cyber Command (ARCYBER), partnering with them "to conduct crime prevention surveys of the Army's LandWarNet to proactively identify vulnerabilities and prevent unauthorized access, misuse, damage and disruption to military operations." During the 2013-2014 period, the crime prevention surveys of LandWarNet resulted in an over $60 million cost avoidance for the Army. The CCIU has also expanded, opening a Hawaii office in July 2013, in accordance with the DoD's new focus on the Asia-Pacific region.[11]

The Major Procurement Fraud Unit (MPFU) investigates financial crimes and corruption related to contingency operations around the world. The MPFU is heavily active in Afghanistan and Kuwait, with four forward-operating investigative offices. These offices look into contractual fraud involving operations under the umbrella of Operation Enduring Freedom and Operation New Dawn. During the period of 2013-2014, the MPFU initiated over 400 Reports of Investigations (ROIs), over 50 of which were in regard to Overseas Contingency Operations

[10] "U.S. Army Center of Military History Department of the Army Historical Summary (DAHSUM), FY 2013," U.S. Army Criminal Investigation Command, August 14, 2014, 7; "U.S. Army Criminal Investigation Command 2014 Spring Semi-Annual Report to Congress," U.S. Army Criminal Investigation Command, 2014, 2-3.

[11] Quotes and information from "2014 Spring Semi-Annual Report to Congress," 3; see also "DAHSUM, FY 2013," 7-8.

(OCO). 2014 was MPFU's most productive year on record and saw the largest single recovery the unit has ever completed. This will be further discussed in Chapter 4.[12]

(b) (6), (b) (7)(C), (b) (7)(E)

CID is the executive agency for the DoD Criminal Investigative Task Force (CITF), "a highly specialized joint unit that conducted criminal investigations of suspected terrorists, war criminals and insurgents, in conjunction with deployed battalions, leading to trials across all appropriate legal venues, including military commissions, U.S. federal courts and host-nation courts." CITF relies on a unique A-3 system: analyst, agent, and attorney. Analysts provide information for Army Ranger battalions and other special operations forces. CID agents are then deployed with these forces, working alongside them and performing sensitive site exploitation. The evidence recovered from these locations is provided both back to the analysts—for use in developing further intelligence and targeting packages—as well as to DoD attorneys who utilize the evidence to ensure trials of captured criminals can be completed appropriately and completely. Originally a joint operation between CID and other MCIOs, CITF realigned into a fully Army unit and is now part of the 701st MP Group. More on its specific missions will be discussed in Chapter 4.[14]

---

[12] Mr. (b) (6), (b) (7)(C) USACIDC, interview with (b) (6), (b) (7)(C) and Dr. (b) (6), (b) (7)(C) Quantico, VA, April 14, 2015, 1-7; "DAHSUM, FY 2013," 8; "2014 Spring Semi-Annual Report to Congress," 3-4.

[13] "DAHSUM, FY 2013," 4.

[14] "DAHSUM, FY 2013," 13-15; "2014 Spring Semi-Annual Report to Congress," 12-23; MG (b) (6), (b) (7)(C) interview, 11-12.

There is another critical element of CID based in Quantico: the U.S. Army Crime Records Center (USACRC, or just CRC). This body is responsible for housing, protecting, and releasing all records pertaining to Army law enforcement investigations. Not only serving the Army and CID, it also provides information to the public through the Freedom of Information Act (FOIA) and to other law enforcement agencies at the federal, state, and local levels, as well foreign agencies when necessary. Housing more than 2.5 million reports, the CRC has many responsibilities and answers approximately four thousand FOIA requests each year. Furthermore, the CRC also oversees the Army Law Enforcement Polygraph Program.[15]

Beyond Quantico, CID has a presence across the country and across the globe. The 3rd Military Police Group (CID) is based at Hunter Army Airfield in Savannah, GA and commanded by COL (b) (6), (b) (7)(C). Prior to June 2014, 3rd MP Group was commanded by COL (b) (6), (b) (7)(C) who is now the Inspector General for U.S. Army Forces Command (FORSCOM) at Ft. Bragg, NC. The 3rd MP Group oversees five subordinate battalions: the Washington Battalion (CID) at Fort Myer, VA, the Ft. Benning Battalion (CID) at Ft. Benning, GA, the 10th MP Battalion (CID) at Ft. Bragg, NC, the 502nd MP Battalion (CID) at Ft. Campbell, KY, and the 5th MP Battalion (CID) in Kaiserslautern, Germany. The Group assists in the various duties and activities of CID, including criminal investigations, protective services, and deploying to combat zones. Its area of operations includes the eastern United States and Canada, the Caribbean, much of Central and South America, Southwest Asia, Europe, and

[15] Ms. (b) (6), (b) (7)(C), USACIDC, interview with (b) (6), (b) (7)(C), March 30, 2015, 1-3; "DAHSUM, FY 2013," 5.

Africa. The 3rd MP Group is also primarily responsible for the active combat theaters in the Middle East.[16]

The 6th Military Police Group (CID) is the other primary extension of CID activity, based at Joint Base Lewis-McChord, WA. Similar to 3rd MP Group, this Group also investigates serious crimes and other sensitive matters on behalf of the Army, as well as deploying to combat situations. The 6th MP Group oversees three subordinate battalions: the 22nd MP Battalion (CID) also located at Lewis-McChord, the 11th MP Battalion (CID) located at Ft. Hood, TX, and the 19th MP Battalion (CID) located at Schofield Barracks, HI. Its area of operations includes the western United States and Canada, Mexico, East Asia, Southern Asia, and Oceania. The current commander of 6th MP Group is COL (b) (6), (b) (7)(C) His predecessor was COL (b) (6), (b) (7)(C) who served as 6th MP Group commander from July 2011 to July 2013.[17]

Prior to July 2013, there was an additional CID Group, the 202nd Military Police Group (CID), headquartered in Stem Kaserne, Seckenheim, Germany. This Group was responsible for CID investigations in the European theater, including two subordinate commands: the 1002nd MP Battalion (CID) based in Bamberg, Germany and the 5th MP Group (CID) based in Kaiserslautern, Germany. Due to overall Army downsizing, the 202nd was redesignated; its headquarters was dissolved and the 1002nd MP Battalion was deactivated. The region now falls within the responsibility of 3rd MP Group. Most of the functional capabilities of the 202nd were

[16] COL (b) (6), (b) (7)(C) U.S. Army, phone interview with (b) (6), (b) (7)(C) and Dr. (b) (6), (b) (7)(C) December 15, 2014, 1-2; "Command Brief," slides and accompanying information, U.S. Army Criminal Investigation Command, June 5, 2014, slides 7-9; "DAHSUM, FY 2013," 3-4.

[17] "Command Brief," slides and accompanying information, U.S. Army Criminal Investigation Command, June 5, 2014, slides 7-9; "DAHSUM, FY 2013," 3-4; "6th Military Police Group," U.S. Army Criminal Investigation Command, http://www.cid.army mil/6thcommander html; Surveillance Photos (4 of 12)," *The Shield*, January 2014.

maintained in the 5th MP Battalion, which remained in Kaiserslautern under the command of 3rd MP Group. More information about the dissolution of the 202nd will be discussed in Chapter 2.[18]

Apart from its specialized units, MP groups, and joint task forces, CID also has other important organizational units that are critical to their goals. Primary among these is the Defense Forensic Science Center (DFSC) at Ft. Gillem in Forest Park, GA. As "the only full service forensic laboratory in the DoD," the DFSC supplies forensic laboratory services for the Department of Defense, its investigative agencies, and other federal law enforcement agencies. The facility oversees CID criminalistics and visual information programs and provides the Special Agent Laboratory Training Course for investigators from all branches of the military. The DFSC consists of many sections, including the U.S. Army Criminal Investigation Laboratory (USACIL)—the primary forensic testing section utilized by CID—along with the Office of the Chief Scientist (OCS) and the Forensic Exploitation Directorate (FXD). The FXD in turn contains the Global Forensic Exploitation Center (GFXC) and Forensic Exploitation Teams (FXTs). These various groups process many different kinds of forensic evidence from a variety of sources. The FXTs can even be deployed in-theater to provide forensic services on the front lines.[19] More on the different sections of DFSC will be discussed in Chapters 3 and 4.

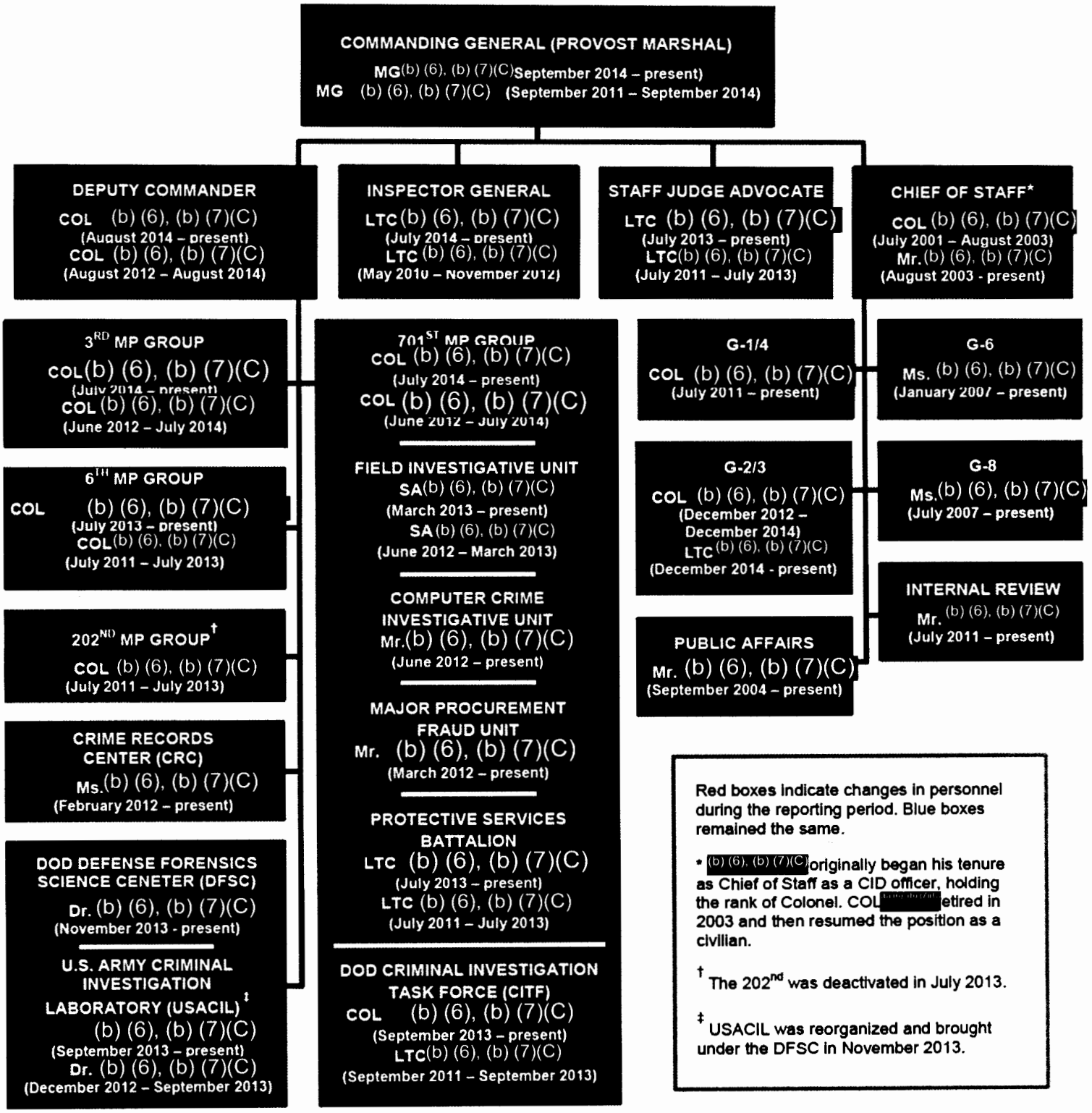
CID's structure has changed significantly during the reporting period, though its mission has remained the same. Much of this restructuring is the result of new policies from the federal government and the Department of the Army. The details of CID policy changes will be discussed in the next chapter.

---

[18] (b) (6), (b) (7)(C), "202nd Group Redesignated," *The Shield*, July 2013; COL (b) (6), (b) (7)(C), USACIDC, interview with (b) (6), (b) (7)(C) and Dr. (b) (6), (b) (7)(C), Quantico, VA, September 18, 2014, 2-4.

[19] "DAHSUM, FY 2013," 4, 8-11; "2014 Spring Semi-Annual Report to Congress," 4-5.

Fig. 1, CID Command Structure



Chapter 2: Policy & Procedure

"In an Army that is coming down, you either show your value—and it is not a time to be modest—you either show your value, or you will be cut."[20] MG (b) (6), (b) (7)(C) statement reflects the changing times that the Army has entered over the past several years. As the conflicts in Iraq and Afghanistan have come to a close, the Army is moving away from operations and policies geared towards active theater combat. The shift in focus must be towards peacetime, as well as preparing for future conflicts. During the period of 2013 to 2014, CID has experienced this transition through a number of changes in policy and procedure. Much of this change has been driven by outside forces: Congress, the DoD, and senior Army leadership. Financial struggles and the end of active combat have led to overall Army downsizing. The command has reacted by reorganizing, restructuring, and adjusting its policies to compensate for these changes. CID has worked to demonstrate its value, meeting the challenges that have presented themselves.

The rigors of an active theater require a great deal of preparation and a different mentality than on the home front. CID battalions, as they prepared to deploy in support of Operation New Dawn and Operation Enduring Freedom, went through a series of training initiatives to ready themselves. Special agents needed to be ready for anything they could face on the battlefield—a much different environment than their garrison investigations. The multiple phases of training include a wide range of exercises and scenarios at several different locations. The Joint Readiness Training Center (JRTC) at Ft. Polk, LA and the 22nd MP Battalion (CID) at Joint Base Lewis-McChord were two of the training sites for a number of CID detachments. CID agents preparing to deploy in 2013 also went through training at two new centers: the Combined

[20] MG (b) (6), (b) (7)(C) interview, September 26, 2014, 4.

Training Center at Ft. Polk and the Federal Law Enforcement Training Centers (FLETC) in Brunswick, GA.[21]

However, CID did not lose its original investigative function when deployed. In fact, as the conflicts in Iraq and Afghanistan began to draw down, CID's law enforcement approach was a crucial asset. To deal with the nontraditional aspects of these conflicts and help establish rule of law, CID supported various missions suited to their skills including investigating prisoners, processing intelligence, and training local authorities about law enforcements techniques. A prominent example is the actions of the 22nd MP Battalion (CID), which supported five such nontraditional initiatives in Afghanistan during 2012.[22]

Part of why CID was so crucial in these operations is because they do not think or operate in the same way as the rest of the Army, or the intelligence community as a whole. These bodies think in terms of defeating the enemy, of targets and networks that must be found and eliminated. CID, as a law enforcement agency, has a different view. Although they also see targets and networks, they focus on prosecution and the legal ramifications of Army actions. Another significant, connected factor is the management of prisoners, which in an active theater can become difficult. In the words of MG [redacted] about his time in Iraq, the problem "was people just dropping bad guys at our gates. We didn't know what...they did. So, what do we do with this guy? I mean, he's got no paperwork, no statements. We do not know whether this guy is Al Qaeda, [or] if he just was in a wrong place at the wrong time. We had no idea."[23]

---

[21] MAJ [redacted], "CID on the move: Units prepare for deployment with combined exercises," *The Shield*, May 2011; COL [redacted] interview, December 15, 2014, 3; CPT [redacted] "502nd MP Bn (CID) Prepared for Deployment," *The Shield*, February 2014.

[22] SA [redacted], "Gray Side Operations," *The Shield*, April 2012.

[23] MG [redacted] interview, September 26, 2014, 10-11.

The confluence of these two issues created a significant problem for the Army, and CID specifically, as in-theater operations drew down. CID's law enforcement skills were vital tools to addressing these issues. The solutions included the use of expeditionary forensics and the integration of CID personnel, such as CITF specialists, with other Army units. A primary example of this drive was the evolution of the Criminal Investigative Task Force (CITF), which placed CID agents with Ranger battalions to process crime scenes during their operations.[24] More on these initiatives will be discussed in Chapters 3 and 4.

CID was also affected by federal government and Army policies off the battlefield as well. Foremost among these were budgetary constraints. Congress, operating under a series of continuing resolutions, has disrupted the budgeting process for essentially the entire U.S. government—the Army and CID included. FY13 began under a continuing resolution with Operation and Maintenance, Army (OMA) funding approximately $6 billion less than requested, a shortfall which in turn increased another $4.6 billion when Sequestration began March 1, 2013. The resource draw of Afghanistan was also larger than anticipated, with a $7-8 billion shortfall in OCO funding. The Army was forced to look for ways to save money by reorganizing their own finances. Subsequent legislation, including the Consolidated and Further Continuing Appropriations Act of 2013 (P.L. 113-6), The Bipartisan Budget Act, and the Consolidated Appropriations Act of 2014, each provided some relief to the OMA budget and allowed FY13 funding continue into the start of 2014. Nevertheless, these shortfalls and the subsequent shuffling of funds have caused a number of negative effects on the Army and CID, such as the reduction of imminent danger pay.[25]

---

[24] MG [redacted] interview, September 26, 2014, 13.

[25] COL (b) (6), (b) (7)(C), "Fiscal Year 2013 (FY13) Operation and Maintenance, Army (OMA) Funding Letter," Department of the Army memorandum, May 13, 2013; COL (b) (6), (b) (7)(C), "Fiscal Year

On a larger scale, the withdrawal from active combat and the budgetary struggles have resulted in significant Army downsizing. Under the initiative of Grow the Army, the size of the force swelled over the late 2000s to meet the demands of Global War on Terrorism (GWOT) operations. By FY14, the Army stood at almost 550,000 strong, but then needed to be reduced as active operations decreased. Total Army Analysis (TAA), in line with Congressional direction, has scheduled the Army to reduce its total strength to 490,000 by FY15, with further reductions to 450,000 by FY17 and 420,000 by FY19.[26] CID is currently in a difficult situation. CID had done some recent reorganization of their Groups in compliance with the Army drawdown, such as the deactivation of the 202nd, which will be discussed later in this chapter. However, they were able to preserve most of the authorizations from the European theater, and were given additional authorizations they had previously requested. This had allowed them to grow recently, though they are facing significant cuts to positions in the comings years, especially FY16 and '17. They now have a "bubble" of authorizations, positions that they can now fill but will be cut within the next few years, which presents some serious problems which will be examined below.[27]

Lack of consensus in Congress also resulted in a government shutdown in October 2013. This in turn had significant effects on CID, and the Army and government as a whole. Initial impacts to CID included several furloughs for non-essential personnel, in addition to a six day furlough during the summer of 2013 for nearly all employees caused by Sequestration. CID's

---

2014 (FY14) Operation and Maintenance, Army (OMA) Funding Letter," Department of the Army memorandum, February 27, 2014; Ms. (b) (6), (b) (7)(C) USACIDC, interview with (b) (6), (b) (7)(C) Dr. (b) (6), (b) (7)(C), and Dr. (b) (6), (b) (7)(C) Quantico, VA, October 17, 2014, 3-5; News Brief, "20 areas lose imminent danger pay," *The Shield*, April 2014.

[26] (b) (6), (b) (7)(C), "Current Manpower and Force Structure Actions," USACIDC Information Paper, January 17, 2014, 1; (b) (6), (b) (7)(C), "Current Manpower and Force Structure Actions," USACIDC Information Paper, July 31, 2014, 1; Mr. (b) (6), (b) (7)(C), USACIDC, interview with (b) (6), (b) (7)(C), Quantico, VA, October 3, 2014, 2; ARNEWS, "Army Supports Soldiers as it Navigates Drawdown," *The Shield*, September 2014.

[27] Ms. (b) (6), (b) (7)(C), October 17, 2014, 6-7; Mr. [redacted] interview, October 3, 2014, 2-3.

Human Resources staff did their best to limit the effects, implementing the furloughs with as little disruption to operations as possible. The civilian staff was the hardest hit, and though most employees eventually received back pay, the ordeal was still a major blow to morale across the command.[28] Between furloughs and lack of funding, CID—and the Army by extension—had difficulty fulfilling their normal duties. Budgeting in particular was an issue, as the inflow of money was unevenly dispersed throughout the fiscal year, throwing off timetables and scheduled spending. Nevertheless, CID managed to meet its budgetary deadlines and markers for FY14, though not without significant effort.[29]

The tightening of funds and the ensuing backlog resulted in the minimizing of many CID programs. Training, travel, conferences, and new initiatives were greatly reduced or halted. A hiring freeze was put in place. Equipment purchasing, along with cataloguing and dispersing of equipment, was drastically cut. Even daily responsibilities were hard to meet, as various sections of the DA staff required each part of CID to report on the effects of Sequestration. Once the government shutdown was over, CID had to scramble to recover and catch up on the lost time. Bogged down by reports and trying to maintain their normal responsibilities, CID activities were delayed weeks or even months. New initiatives were halted and had to be picked up again later, if at all.[30]

Beyond these initial impacts, Sequestration will have ripple effects in the future. Due to the disruption of furloughs and the budgetary issues surrounding the government shutdown, the

---

[28] Ms. (b) (6), (b) (7)(C), October 17, 2014, 3; COL (b) (6), (b) (7)(C), USACIDC, interview with [redacted] and Dr. (b) (6), (b) (7)(C), Quantico, VA, October 8, 2014, 4; COL (b) (6), (b) (7)(C) interview, December 15, 2014, 3; Mr. [redacted] interview, October 3, 2014, 3-4, COL [redacted] phone interview, April 6, 2015, 3-4.

[29] Mr. [redacted] interview, October 17, 2014, 2-3; Ms. (b) (6), (b) (7)(C), October 17, 2014, 3-4.

[30] Ms. (b) (6), (b) (7)(C), October 17, 2014, 4; CCWO (b) (6), (b) (7)(C), October 24, 2014, 7; COL (b) (6), (b) (7)(C) interview, October 8, 2013, 4; Ms. (b) (6), (b) (7)(C), USACIDC, interview with (b) (6), (b) (7)(C), Quantico, VA, September 24, 2014, 3; COL (b) (6), (b) (7)(C) interview, April 6, 2015, 3-4.

Department of the Army has chosen to recoup their losses in another way, primarily through cuts in position authorizations. These reductions work in tandem with the aforementioned Army drawdown. While CID has yet to feel the impact of these cuts, during the span of FY16 through FY19 there will be a series of reductions. While many of the cuts across the command have been mitigated by rearranging authorizations or through temporary measures, the hardest hits will be at the Headquarters in Quantico. Creating authorizations at Headquarters have been more difficult than for many of the operational units. Given its already lean size, any cuts to the staff there are significant.

With the transition out of wartime, the Secretary of Defense mandated at twenty percent cut in headquarters all across the DoD. The Secretary and Chief of Staff of the Army in turn ordered a twenty-five percent reduction to all two-star headquarters and above. CID, as a two-star headquarters, will thus be affected, despite its size. Unlike most other headquarters, CID remained comparably very small and did not expand during combat operations in the Middle East. The reductions mean various responsibilities will have to be shuffled around and reassigned to compensate, as many singleton positions—such as the safety officer and engineer—will likely be cut. Furthermore, only two-thirds of CID Headquarters performs normal headquarters responsibilities. The remaining third carries out operational support, such as accreditations, standards of conduct, operational policy, and more. In the words of (b) (6), (b) (7)(C), CID Chief of Manpower, the combination of Army downsizing and strain from Sequestration results in drastic reductions:

> What this means for CID command is it equates to—as far as Sequestration or the Budget Control Act—a ninety-seven space cut of which ninety-seven are civilian and then another eight military. This is in addition to the forty-one civilian space reductions in '16 and '17 as a result of Grow the Army, the proportioned civilian reduction following the military reduction from 547 to 490k. So, that translates to a 146-space cut for CID to be spread from '16 through '19. And it is probably most impacted in our Headquarters,

> where we are taking a twenty-one percent cut, sixteen civilian and eight military. That is pretty tough, because the Manpower Analysis Agency did a manpower study of our Headquarters and validated 128 requirements. Of that, we have 113 authorizations, so we are already operating at a deviation between what our workload is to what our sourced authorizations are. At end state, what this reduction does is brings that 113 down to eighty-nine authorizations for a total of thirty percent reduction.

The twenty-one percent cut is a compromise, as there is some understanding from senior leadership that CID is valuable and is already a lean force. Nevertheless, reductions will have to be made, though their full extent is still uncertain.[31] More on specific growth and cuts will be discussed in Chapter 3.

In addition to budgetary legislation, CID has been subject to a number of legal changes over the course of 2013 and 2014. Much of this legislation has been focused on the issue of sexual assault. Article 120 of the Uniform Code of Military Justice (UCMJ) defines the scope of sexual assault, which has been expanded in the last few years. Encompassing more than rape, sexual assault in the eyes of the Army includes any kind of unwanted sexual contact. This is a much broader definition than that of other law enforcement agencies, which in turn allows CID to investigate crimes that local or state authorities would not. The 2014 National Defense Authorization Act (NDAA) set a number of additional requirements for CID in regards to their investigations of these crimes. Previously, there had been a five year statute of limitations on sexual assault related crimes. Under the new law this statute has been lifted, prompting victims to come forward and allowing CID to pursue a spate of previously uninvestigated crimes.[32] Furthermore, the NDAA put forth new requirements for the collection and retention of evidence in relation to sexually related crimes. All evidence in such cases must be kept for at least five

[31] Quote and information from Mr. [redacted] interview, October 3, 2014, 3-5. Additional information from Mr. [redacted] USACIDC, interview with [redacted] Dr [redacted], and Dr [redacted] Quantico, VA, October 17, 2014, 3-4; COL [redacted] interview, October 15, 2014, 6-8; [redacted] "Current Manpower and Force Structure Actions," July 31, 2014, 1.

[32] LTC [redacted] USACIDC, interview with [redacted], Quantico, VA, October 3, 2014, 3-7.

years. This often includes a digital or technological component, such as a smart phone. CID has taken action to accommodate this change, including the expansion of a number of evidence warehouses. One such facility underwent extensive expansion at Hunter Army Airfield, GA to support 3rd MP Group, while the Consolidated Evidence Long-Term Storage Facility opened at the end of 2014. This facility is the first of its kind within CID.[33]

Another important change was the expansion of the Special Victim Counsel Program, which assigns a specially trained lawyer to represent any victim of a sexual assault. CID policies had to adjust to account for this new legal representation for victims without obstructing their investigations or inhibiting the collection of critical evidence. Overall, these legal changes have made CID tailor and specialize their policies and procedure to ensure that sexual assault cases are handled efficiently and professionally. The NDAA also includes further changes to the reporting of such crimes, bringing them to trial, the handling of cases within a court-martial, the punishment of convicted parties, and protection of victims. Significant changes include that victims can elect not to testify, that victims can receive monetary restitution, that any soldier convicted of sexual assault cannot continue to serve in the Army (with a guilty verdict resulting in dismissal or dishonorable discharge), and that rank and service record must have no bearing on the outcome of a trial.[34]

Apart from the various external policies that have steered CID during the past two years, there have also been a number of internal changes. From a legal standpoint, CID operations are directed by the 195-series regulations, which cover law enforcement; Regulation 195-1

---

[33] COL (b) (6), (b) (7)(C) interview, December 15, 2014, 2-4; LTC [redacted] interview, October 3, 2014, 3-4; CSM (b) (6), (b) (7)(C) interview, October 15, 2014, 7; "Consolidated Evidence Long-Term Storage," *The Shield*, December 2014.

[34] LTC [redacted] interview, October 3, 2014, 3-4; CCWO [redacted] interview, October 24, 2014, 3; CPT (b) (6), (b) (7)(C), "Prosecuting Sexual Assault Gets a Boost With the 2014 NDAA," *The Shield*, June 2014.

encompasses most of its policies and procedures. Due to the nature of the regulations and CID's operations, these regulations are continuously in flux. Incremental changes are made essentially on a daily basis, regarding everything from personnel requirements to investigation procedures. The Judge Advocate staff maintains and monitors changes to the 195-series and advises the command as to these alterations. Different sections of CID must then be vigilant to ensure that they are in compliance with the regulations, such as the Accreditations Division, which must constantly watch for changes in agent credentials.[35]

Apart from legal changes, the most predominant shifts were changes in leadership and organization. Changes of command are relatively routine in the Army, though CID experienced a period of relative stability during most of the reporting period. MG [redacted] was CG of CID from September 2011 to September 2014 and COL [redacted] occupied the position of DCO from mid-2012 to mid-2014. Together they represented a temporary sense of consistency among the continuous rotating of positions. In the summer of 2014, COL [redacted] replaced COL [redacted] as DCO and soon after MG [redacted] the position of Provost Marshal and CG of CID, causing a major turnover of CID leadership. The stability for several years prior allowed for a united front to move forward on numerous initiatives. Furthermore, the Chief of Staff, [redacted] has held the position since 2001. His presence has provided another level of balance and continuity during the shifts in leadership among the rest of the command group.[36]

One of the most significant changes to the structure of CID was the deactivation of the 202nd MP Group. The decision to deactivate the Group, along with the 1002nd MP Battalion, was driven by the overall Army drawdown and the new DoD focus on the Pacific Rim. Planning for

---

[35] LTC [redacted] interview, October 3, 2014, 4; COL [redacted] interview, October 8, 2014, 4.

[36] MG [redacted] interview, September 26, 2014, 1-2, 23-24; COL [redacted] phone interview, April 6, 2015, 1-2, 5-6; COL [redacted] interview, October 15, 2014, 1-6; [redacted] interview, October 17, 2014, 1-5.

the dissolution of the 202nd began in mid-2012, followed by meetings between the leadership of the 202nd and 3rd MP Group, which would assume command over the European theater. The Battalions began reporting to 3rd MP Group during early 2013; each office was transferred over one at a time. It was a gradual process, culminating with the final deactivation ceremony on June 30, 2013. Starting July 1st, the 202nd and the 1002nd were officially deactivated.

Although some difficulties were to be expected, the transition was relatively smooth, with continuous operational capability throughout. There were some adjustments changing from a self-contained Group to a single Battalion reporting to a distant headquarters. However, such a move was not unprecedented. CID had previously withdrawn most of its forces from Europe, only to reverse their decision and reactive the "Second Region" and form the 202nd in 1996. Whether this reorganization of European forces will last is up for debate. Nevertheless, CID managed to accomplish this major change in structure with little to no loss of operational ability.[37]

The dissolution of the 202nd had many benefits for CID. In the view of MG (b) (6), (b) (7)(C) it made CID a more efficient organization. With Army downsizing, maintaining the Group in Europe was not practical or particularly necessary, as proportionally there is less crime in that region than most other areas of CID responsibility. By reducing the Group and two Battalions to the lone 5th MP Battalion, CID was able to reduce their surplus footprint in Europe and save the authorizations to use elsewhere. Twenty seven authorizations were taken from the dismantling of the Group headquarters and redistributed throughout the command, specifically filling shortfalls for the PSB and other manpower-intensive personal security missions. As far as resource

[37] COL (b) (6), (b) (7)(C) interview, December 15, 2014, 1-2; CCWO [redacted] interview, October 24, 2014, 1-2; Mr. [redacted] interview, October 3, 2014, 2; Mr (b) (6), (b) (7)(C), October 17, 2014, 3; COL [redacted] phone interview, April 6, 2015, 3; (b) (6), (b) (7)(C) "202 Group Redesignated," *The Shield*, July 2013.

management, the deactivation resulted in some extra work for the 3rd MP Group as they sorted out their new responsibilities, though the simpler organization and fewer reporting bodies will help in the long run. Additionally, there were some modest financial savings from only funding a Battalion over an entire Group and its subordinate commands. In terms of logistics and equipment, great care was taken to ensure that all supplies were redistributed as needed, including the use of a barcoding and scanning system. This allowed CID to fill in gaps in their logistics chains much as they did with personnel, which in turn saved additional money.[38]

Having the 5th MP Battalion be responsible for all of Europe still presents challenges. In the words of COL (b) (6), (b) (7)(C) former commander of 5th MP Battalion, the question was "How are we going to do everything that the Group does? How are we going to execute the mission…to the same standard that we did out of Group Headquarters in Europe?" For the most part, the investigative capacity of CID was not diminished by the dissolution of the 202nd, as much of that capability was transferred to 5th MP Battalion. Nevertheless, there was a great deal of adjustment to ensure that the Battalion was able to oversee all of Europe. One example of a function that had to be transferred was local legal support. Prior to deactivation, there was a German attorney based out of the 202nd headquarters who proved legal advice and guidance with regards to German law. The 5th MP Battalion did not have this specialized function, and the position had to be moved to compensate. The scope of the Battalion increased dramatically, overseeing offices in Germany, Belgium, Italy, and Kosovo.[39]

The United States Army Criminal Investigation Laboratory (USACIL) was another section of CID to take on new responsibilities. Over the course of many years, it has expanded

[38] MG [redacted] interview, September 26, 2014, 8; Mr. [redacted] interview, October 3, 2014, 2; Ms. [redacted] interview, October 17, 2014, 9; Ms. [redacted] interview, September 24, 2014, 7.

[39] COL [redacted] interview, September 18, 2014, 2-3; "5th Military Police Battalion (CID)," U.S. Army Criminal Investigation Command, http://www.cid.army.mil/5th.html.

both its capabilities and its duties to the DoD and many other organizations. As of November 13, 2013, USACIL was redesignated as the Defense Forensic Science Center. The name "USACIL" is still used, but only in reference to the part of the DFSC that specifically handles forensic evidence tests, such as DNA and fingerprints. The DFSC now has multiple other sections, including a mission support section, a research and program management section, and an expeditionary forensics section. This last responsibility is of particular interest, as expeditionary forensics is a new and growing area. Although it had expanded greatly during wartime, the funds for such capabilities are now dwindling. Nevertheless, the DFSC is maintaining as much of those abilities and personnel as it can. There has been a great deal of training involved to build a competent and professional staff.[40]

Training and Forensics have been other sources of change for CID in the last several years. The Forensic Science Master's Program is the established method for a warrant officer to become certified as a Forensic Science Officer for CID. This certification provides a warrant officer with the necessary skills to effectively process a crime scene and handle various kinds of evidence. For many years, the Master's program was operated through George Washington University in Washington, D.C. The university originally had strong ties to the Armed Forces Institute of Pathology (AFIP), which was also in the capital. While the warrant officers went through the program, they also completed a year-long medical research fellowship through AFIP. Over time, AFIP was broken up into multiple sections and largely disbanded. The Armed Forces Medical Examiner's Office (AFME) also moved from the Washington, D.C. area, ultimately ending up at Dover Air Force Base, MD. As a result, George Washington University lost its previous connections with these bodies. Though students in the Forensic Science program could

[40] (b) (6), (b) (7)(C), "USACIL now the Defense Forensic Science Center," *The Shield*, December 2013; Mr. (b) (6), (b) (7)(C) interview, October 17, 2014, 3.

still complete their fellowship, the distance to Dover was prohibitive and most students did not work on them concurrently. The military doctors from AFIP and AFME no longer taught classes at George Washington. Additionally, the cost of tuition for the university was steadily increasing.

(b) (6), (b) (7)(C) a veteran of CID and an alumnus of the George Washington program himself, became the Command Forensic Science Officer in October 2013. Seeing the issues with the Forensics Science Master's Program, he wrote a decision paper to address these problems. George Washington was no longer the only institution with a reputable forensics program, as it had been at the program's inception. [redacted] found a promising program at George Mason University. George Mason had many advantages over George Washington, including classes in Forensic Anthropology, guest lectures from the State Forensic Anthropologist, visits to active dig sites, internships with the State Medical Examiner, and new technology and equipment. George Mason also offers a Master's program in digital forensics in addition to physical forensics, allowing FSOs to be trained in the much needed field of digital forensics. On top of that, George Mason is a public university while George Washington is private. The cost of sending two students (the standard number) through the Master's program at George Washington was $104,000. George Mason offers in-state tuition to military personnel, meaning that five students could complete their program for only $97,000.

MG (b) (6), (b) (7)(C) approved the switch to George Mason in 2014, and the first two CID officers were sent to the Master's program soon after. Starting in 2015, the full five will be able to start the program, with each group split between physical and digital forensics. The new program is showing great progress and the students have provided positive feedback about the change. Other MCIOs are also showing interest in George Mason. The Air Force Office of Special Investigations (OSI) sent a forensics student along with the first pair of CID officers. OSI

had stopped using George Washington many years prior, opting to take online classes with the University of Florida in conjunction with lab training. If the feedback continues to be good, then OSI may switch to George Mason in the near future.[41]

In addition to this broadening of forensic training to warrant officers, enlisted CID agents have also been presented with a new training program. The Forensic Science Technician (FST) program is a new class and certification that expands an agent's forensic knowledge and crime scene processing skills. The training consists of a four-week intensive training program run by 3rd MP Group. The first two weeks of the course are taught at the Military Police School for Advanced Crime Scenes at Ft. Leonard Wood, MO, followed by two weeks at FLETC in Georgia. Though not as extensive as the Forensic Science Master's Program, it nevertheless provides a strong boost to an agent's capability to fully exploit a crime scene. The program certifies the FSTs as Level 1 Crime Scene Investigators as set by the International Association for Identification. It also certifies them to use certain technology and equipment, such as the Faro scanner, a machine that creates a three-dimensional recreation of a crime scene.[42]

In addition to new training initiatives, both warrant officers and NCOs were drastically affected by the restructuring of CID detachments. One of MG (b) (6), (b) (7)(C) early command goals was to redesign the traditional two-agent team into a three-agent team. For many years, the standard CID team consisted of a single NCO and a single warrant officer. The one to one ratio of warrant officers to NCOs created a shortage of warrant officers, and it was very difficult to develop more as the base of NCOs was small in comparison. Starting in FY15, MG (b) (6), (b) (7)(C)

[41] Mr (b) (6), (b) (7)(C), USACIDC, interview with (b) (6), (b) (7)(C) and Dr. (b) (6), (b) (7)(C), Quantico, VA, October 15, 2014, 1-2, 9-10; (b) (6), (b) (7)(C) "Forensic Science Program Moves," *The Shield*, April 2014.

[42] (b) (6), (b) (7)(C) interview, October 15, 2014, 3-4; CSM (b) (6), (b) (7)(C) interview, October 15, 2014, 4-5; COL (b) (6), (b) (7)(C) phone interview, December 15, 2014, 6-7; (b) (6), (b) (7)(C), "Forensic Science Technician Training," *The Shield*, April 2014.

changes take effect and each team will consist of two NCOs under a warrant officer. The reorganization converted sixty-four officer positions to enlisted status, reducing the number of total warrant officers. However, the change will help warrant officers to grow in the long term, building a foundation for future warrant officers. Furthermore, the smaller number of warrant officer slots makes the field more competitive, driving better candidates to fill those positions.[43]

The second major change to CID detachments was the growth from twenty-one soldiers to twenty-six which began October 1, 2014. The additional five positions were not filled by typical 311A warrant officers or 31D NCOs, but by 31B "Bravo" combat support MPs. MG [redacted] proposed the use of MPs to help fill manpower gaps in CID operations, as well as to save MP authorizations which were scheduled to be cut due to Army downsizing. As Provost Marshal, he authorized the loaning of the 31Bs for a provisional period until the positions were officially authorized as part of a TAA. The MPs have been attached to Drug Suppression Teams (DSTs), which are in high demand due to the rise in drug-related crime. However, Bravos have also been added to the PSB and personal security missions. Their presence and combat support experience is a major asset, because this mission is manpower intensive and is often filled with less experienced agents.[44] More on DST and PSB operations will be discussed in Chapter 4.

As the detachments have been redesigned, there have also been policies and programs regarding the careers of agents, including recruiting, accession, and attrition. CID recruitment has undergone several important changes during the reporting period. In recent years, the applications rates to CID had fallen and the operational focus—particularly with continued

---

[43] MG [redacted] interview, September 26, 2014, 8-9; CCWO [redacted] interview, October 24, 2014, 4-5; CSM [redacted] interview, October 15, 2014, 7.

[44] "DAHSUM, FY 2013," 5; MG [redacted] interview, September 26, 2014, 5-6; Mr. [redacted] interview, October 3, 2014, 3, 6; CCWO [redacted] interview, October 24, 2014, 5; CSM [redacted] interview, October 15, 2014, 7.

conflict in the Middle East—had diverted resources away from recruitment. With the withdrawal from overseas, recruitment did not pick back up due to the overall Army drawdown. There was also no specific position in charge of recruitment; it was an additional duty for agents at bases across the world. However, CID has introduced several new initiatives to promote renewed recruitment and accession into CID. The Accreditations Division, in conjunction with the G-6 and the Public Affairs Office (PAO), set up an online application for prospective CID agents, replacing the traditional paper application. Starting July 1, 2014, the new SharePoint portal went live, allowing interested soldiers the ability to apply from anywhere at any time. Rather than the former physical packet, the online application is much easier to complete and submit, and saves time for both the applicant and those reviewing it. The system can automatically reject applications that do not meet the minimum requirements.

To further streamline the application process, a new Recruitment Operations Cell was created to oversee the online system. The Cell consists of three NCOs that do preliminary quality control on incoming applications and assist applicants with the process. This has taken the additional duty of giving briefings and managing packets off the shoulders of forty-six locations that were previously responsible. The centralization of the process, along with streamlining features, has dropped the turnaround time from over six months to about ninety days. The online system has prompted renewed interest in CID, with a flurry of applications arriving once the site was activated. Though the initial rush has begun to taper off, there is still a surplus of applicants compared to open positions for the coming year. As of the start of FY15, there were over 200 potential soldiers for a little over 100 spots. Space is limited and that has its advantages: it makes the pool more competitive and ensures that the best soldiers are accessed into CID.[45]

[45] Ms. (b) (6), (b) (7)(C) USACIDC, interview with (b) (6), (b) (7)(C) and Dr. (b) (6), (b) (7)(C), September18, 2014, Quantico, VA, 5-7, 10-11; Ms. (b) (6), (b) (7)(C), USACIDC, interview with (b) (6), (b) (7)(C) and Dr. (b) (6), (b) (7)(C)

Another method of getting talented individuals into CID is the Direct Accession Program. This pilot program, started in August 2012, finds bright students at universities across the country who are pursuing degrees in appropriate fields (such as criminal justice or forensic science) and offers them immediate entry into CID upon graduation. The usual accession method requires an applicant to first enlist in the Army and then serve for a minimum period of two years before entering CID. Direct Accession allows the students to bypass this requirement, go through preliminary training at USAMPS and the Criminal Investigation Special Agent course, and then start their career in CID. The program can train an apprentice agent and have them enter the CID workforce in only ten months. Originally driven by CSM [redacted] the project was picked up by CSM [redacted] and the Accreditations Division and is now starting to come to fruition. There are currently twenty-two new soldiers scheduled to enter CID in the coming year, with at least five that have graduated from training and have started their apprenticeship at CID. The Direct Accession soldiers are paired with experienced agents, and thus far, the results have been quite promising. The agents are adjusting well to their new responsibilities. The program as a whole has been successful enough that it has been extended beyond its original pilot period for another two years through FY16. If at that point the graduates of the program have continued to do well, it will likely become an official method for accession into CID.[46]

There has also been a significant shift in policy as to how new agents coming from training are assigned to their first posting. The fresh agents go through a probationary period of twelve to eighteen months where they gain firsthand experience as a CID agent, at which point

---

[redacted] October 8, 2014, Quantico, VA, 4; Mr. [redacted] USACIDC, interview with [redacted] and Dr [redacted], Stafford, VA, April 6, 2015, 8-9;COL [redacted] interview, October 15, 2014, 11-12; CSM [redacted] interview, October 15, 2014, 3-4.

[46] Ms [redacted] interview, September 18, 2014, 3-5; CSM [redacted] interview, October 15, 2014, 3-4; [redacted] CID Extends Direct Accession Pilot Program," *The Shield*, July 2014; [redacted], "Like Father, Like Daughter," *The Shield*, November 2014.

they can then be transferred to another position. The original requirement was that this first posting had to be with an investigative detachment. Though useful for ensuring that new CID agents master the basics of investigations, the investigative sections of CID are not necessarily in need of that additional manpower. The specialized units, especially the PSB, are the primary areas in need of personnel. MG [redacted] altered the requirement, allowing these agents to go to the point of need upon completing their training. This not only alleviated the manpower shortages with the influx of new agents, it also streamlined the overall system of transfers and personnel movement. Previously, when each class graduated from training and its students were sent to their initial investigative posts, positions had to be vacated to accommodate them. This required established agents—who had experience with the detachment and region they were in, and who could be in the middle of long-term investigations—to be moved elsewhere. Neither the new agents nor the experienced ones where helped by this shuffling around. Now, fresh agents are directly sent where the manpower is most needed. The PSB has been the main recipient, covering most of its shortfalls. To counteract the relative inexperience of these new agents, and to ensure that not all new agents train in personal security and lack investigative experience, the PSB has been given a large number of 31B MP positions, as discussed previously.[47]

On the other side of personnel affairs—attrition and retention—CID also faces challenges. Attrition rates have remained relatively stable over the last several years, while recruitment rates (until recently) had dropped. As such, CID has to keep up its recruiting and retain as much personnel as possible to continue operating fully, especially with the cuts coming in the next few years. CID must also be competitive with other potential employers. The training and experience of CID personnel can be very valuable for other government or private sector jobs. Still, several of the programs developed in 2013 and 2014 have had a positive impact on

[47] MG [redacted] interview, September 26, 2014, 9-10; Mr. [redacted] interview, October 3, 2014, 6.

retention. The forensics training in particular has been an incentive for many CID agents who have considered leaving the organization. The opening of more slots for the Forensic Science Master's program and the addition of a Digital Forensics Master's has led some warrant officers to stay in CID, hoping to get the degree and either advance in CID or have additional certifications before they retire. Similarly, the FST program has encouraged a number of NCOs to reenlist so they can access that training and gain those certifications.[48]

CID has faced a number of challenges in the last few years and has done much to overcome them. Between Army downsizing and fluctuating finances, CID has compensated for the many changes that have confronted them. They had evolved, and continue to evolve, to carry out their mission. In the words of MG (b) (6), (b) (7)(C) CID has "expanded beyond what we were doing, just Title 10 felony investigations—from trying to prevent crime, to basically breaking up criminal networks, to building cases for prosecution in court… [T]hen trying to make sure that we met the requirements of the division and brigade commanders in theater: sitting on the sexual assault review panels, making sure that they understand what the threats were… So all of that stuff has vastly changed how we employ our forces."[49] These forces, the men and women of CID and the technology and equipment at their disposal, will be discussed in the next chapter.

[48] Ms. (b) (6), (b) (7)(C), September 18, 2014, 8; (b) (6), (b) (7)(C) interview, October 15, 2014, 2; COL (b) (6), (b) (7)(C) phone interview, December 15, 2014, 6-7.

[49] MG (b) (6), (b) (7)(C) interview, September 26, 2014, 13.

Chapter 3: Manpower & Resources

"You got to enable the people that work for you, and you got to create trust up and down and horizontally across your organization. And if you do that, everything else will sort of right itself, because you got a lot of great, smart folks out there that will help you come up with great ideas on how to propel the organization forward," stated MG [redacted] about his philosophy of leading CID. As outlined in the first two chapters, CID has many different sections across the world. Yet their overall footprint is small, only a small fraction of the total Army.[50] Nevertheless, CID pursues its missions, utilizing its combination of military and civilian personnel, its auxiliary sections such as the DFSC, and various technologies. Despite the financial and legislative hurdles discussed in the last chapter, CID has managed its budget in order to grow in the last few years. These numerous resources and acquisitions will be discussed herein.

CID had 2285 authorizations in FY13, 996 in MTOE and 468 in TDA. This was somewhat more than FY12, where authorizations totaled 2145, with a 1104 MTOE/395 TDA split. The growth was primarily in TDA elements, representative of the difficult funding period of 2013 and 2014. CID was able to continue its growth and shift much of that increase to MTOE positions in FY14: total authorizations reached 2512 with 1162 in MTOE and 471 in TDA. The growth was split between a number of military and civilian positions in different areas of the command, though cuts are looming in the future due to Sequestration.

As an MCIO, CID is largely manned by military personnel. Though the civilian staff is critical to carrying out their mission, officers, warrant officers, and NCOs form the backbone of the organization. Almost two-thirds of CID personnel are military, who in turn make up the

[50] Quote and information from MG [redacted] interview, September 26, 2014, 27.

Fig. 2, CID Total Authorizations by Unit, FY12, FY13, & FY14[51]

FY 2012 Authorizations

Unit	Officers	Warrant Officer	Enlisted	Civilian	Total
Headquarters					
701st	4	65	126	256	451
3rd	31	159	250	71	511
6th	36	167	287	79	569
202nd	15	70	144	45	274
USACIL				162	162
CRC		2		52	54
Total	100	480	819	746	2145

FY 2013 Authorizations

Unit	Officers	Warrant Officers	Enlisted	Civilian	Total
Headquarters	14	17	12	103	146
701st	4	78	140	289	511
3rd					361
6th	36	181	296	86	599
202nd					
USACIL				167	167
CRC		2		52	54
Total	94	524	846	821	2285

FY 2014 Authorizations

Unit	Officers	Warrant Officers	Enlisted	Civilian	Total
Headquarters	14	17	12	103	146
701st	4	78	146	316	544
3rd	40	262	508	147	957
6th	36	171	343	94	644
USACIL					
CRC		2		52	54
Total					

[51] (b) (6), (b) (7)(C) "CID Current Force (FY12 Authorizations)," slide, USACIDC Manpower and Force Structure Division; (b) (6), (b) (7)(C) "CID Current Force (FY13 Authorizations)," slide, USACIDC Manpower and Force Structure Division; (b) (6), (b) (7)(C) "CID Current Force (FY14 Authorizations)," slide, USACIDC Manpower and Force Structure Division.

majority of CID special agents (SAs). These agents compose the investigative and operational elements of CID at the core of the organization. The total number of SAs rose slightly from 1371 in FY13 to 1411 in FY14, forming fifty-four percent of all CID authorizations. Most of the growth was among civilian agents, which will be discussed below. The division between warrant officer and enlisted agents is fairly even. In FY13, there were 520 311A Warrant Officers and 570 31D NCOs, with only a growth of six 311As in FY14.[52] This close ratio, as mentioned in Chapter 2, has been addressed by the restructuring of the detachments and the formation of three-person teams put forth by MG (b) (6), (b) (7)(C) which began at the start of FY15.

Military SAs are active duty soldiers who are accepted into CID and must meet the following minimum requirements:

- U.S. citizenship
- Minimum age of twenty-one
- Completed Warrior Leaders Course
- Maximum grade of SGT. SSG (with one year or less time in grade) may apply with waiver
- Minimum of two years of military service and maximum of ten years of military service
- Minimum of sixty college semester hours from an accredited institution
- Minimum Skilled Technical (ST) score of 107 or higher and General Technical (GT) score of 110 or higher
- Consistently meet the height and weight standards prescribed in AR 600-9 and consistently pass the Army Physical Fitness Test
- Ability to deploy worldwide and have no physical limitations
- Normal color vision
- Must possess a valid driver's license and favorable driving record
- Ability to speak and write clearly
- Minimum of one year of military police experience or two years civilian police experience (May be waived for Active duty only)[53]

[52] (b) (6), (b) (7)(C), "CID Current Force (FY12 Authorizations)," slide, USACIDC Manpower and Force Structure Division; (b) (6), (b) (7)(C), "CID Current Force (FY13 Authorizations)," slide, USACIDC Manpower and Force Structure Division; (b) (6), (b) (7)(C) "CID Current Force (FY14 Authorizations)," slide, USACIDC Manpower and Force Structure Division; "Command Brief," slides and accompanying information, U.S. Army Criminal Investigation Command, June 5, 2014, slide 6.

About forty percent of SAs come from the Military Police, having previously served as 31B MPs. Their experience is useful, though SAs are accessed into CID from all areas of the Army. CID Special Agents go through rigorous training upon entering the organization. Each candidate goes through the CID Special Agent Course, a sixteen-week intensive program offered by USAMPS at Ft. Leonard Wood.[54]

To become a CID warrant officer, enlisted SAs must go through another application process and meet additional requirements:

- Meet baseline Army requirements
- Pass all physical test upon entering Warrant Officer Candidate school
- Minimum of two years investigative experience as a 31D Special Agent
- No more than twelve years in the Army (unless waived)
- Graduated from the Advanced Leaders' Course (ALC)
- GT score of 110 or higher
- A bachelor's degree (may be reduced to minimum ninety credit hours on individual basis)
- Clean record of behavior and ethics (as above)

These requirements underwent some minor changes in mid-2014, including the addition of the ALC.[55]

Not all CID soldiers are Special Agents. As of FY 14, there are ninety-four officers in command and support roles, in addition to a large section of military support personnel: four warrant officers and 439 NCOs. Support staff includes the Deputy Chiefs of Staff, legal, and other administrative functions. The Deputy Chief of Staff for Support (G-1/4) is responsible for human resources and logistics for the command. They oversee all military and civilian personnel,

---

[53] Requirements quoted from "Active Duty Enlisted & Reserve Requirements," U.S. Army Criminal Investigation Command, http://www.cid.army.mil/militaryagent2.html.

[54] MG [redacted] interview, September 26, 2014, 5; Ms. [redacted] interview, September 18, 2014, 7-8; "Special Agent Training," U.S. Army Criminal Investigation Command, http://www.cid.army.mil/agenttraining.html.

[55] CCWO [redacted] interview, October 24, 2014, 2-3.

monitoring the strength of the command, hiring, disciplinary action, policy analysis and more. The G-1/4 during the reporting period was COL (b) (6), (b) (7)(C) She oversaw a number of different sections such as the Engineer and Safety Officer. The CID Engineer serves as the liaison with the DA and the Army Corp of Engineers. He oversees buildings and installations across the command, ensuring they are structurally sound and able to be fully utilized, as well as scheduling repairs and maintenance. The CID Safety Officer is an advisor to the CG on safety matters and coordinates with the Army Combat Readiness and Safety Center at Ft. Rucker, AL. He analyzes accident trends and issue warnings and other safety-related information throughout the command, as well as organizing safety training and sitting on a number of safety-related panels. Each of these is only a one-deep position, with no subordinates. Additional sections under the G-1/4 have civilian leads, such as Logistics and Accreditations, and will be discussed in the civilian section.[56]

The Deputy Chief of Staff for Intelligence and Operations (G-2/3) oversees intelligence gathering and analysis as well as strategic planning, investigations, and other ongoing operations. The G-2/3 is primarily responsible for issuing fragmentary orders, officially allocating resources to specific missions and operations, as well as memorandums on policies and regulations. They distribute these orders and messages on behalf of the CG and they carry the commander's authority. The G-2/3 during the reporting period was COL (b) (6), (b) (7)(C).[57] A significant addition under the G-3 was brought into the command in the summer of 2014. COL (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) a forensic psychiatrist, joined CID on June 30, 2014. An experienced officer in both the medical and behavioral fields, COL (b) (6), (b) (7)(C) is the first person to hold such a position within CID. Forensic psychiatry is a growing field in the law enforcement community, and many other

[56] COL (b) (6), (b) (7)(C) interview, October 8, 2014, 1-3.

[57] COL [redacted] interview, September 18, 2014, 1-2.

agencies and even MCIOs have already added such positions to their organizations. As a forensic psychiatrist, COL [redacted] aids the command in a number of ways, including conducting threat assessments for the PSB, assisting interrogations, and performing psychological autopsies. This last function is the examination of the subject of a death investigation to offer mental health insights, such as whether a death was likely a suicide, homicide, or accidental death. Despite being a recent addition to the command, COL [redacted] has integrated strongly into CID and is already busy assisting investigations. He hopes to further strengthen CID's forensic behavioral capabilities, adding more positions and building relationships with related organizations, such as the Center for Forensic Behavioral Sciences at Walter Reed Army Medical Center.[58]

Other important military functions are the CID Inspector General (IG) and Staff Judge Advocate. CID IG provides internal review of the command's operations, ensuring that CID cases are handled properly, fairly, and fully. They find areas in need of improvement and help the command to become stronger and more effective.[59] The current CID IG is LTC [redacted] The Judge Advocate office is responsible for the legal aspects of CID. These lawyers make sure that CID policies and operations meet the regulations put in place by the government and the Army. They provide legal support for operations and the CG—only in his capacity as CG of CID, not as Provost Marshal General—as well as handling issues of agent misconduct. The CG makes the final decision as to whether an agent will be removed from CID or not, though the Judge Advocate soldiers handle processing the case. The current Staff Judge Advocate is LTC [redacted] The Staff Judge Advocate oversees a team of twenty-six, including two officers and two civilian lawyers at Headquarters, five lawyers with 701st MP Group, one with 3rd MP Group, one with 6th MP Group, and one with 202nd MP Group (now the 5th MP Bn).

[58] COL [redacted], USACIDC, interview with [redacted], Quantico, VA, March 30, 2015, 1-8

[59] MG [redacted] interview, September 26, 2014, 16, 21.

There are also two lawyers stationed at the DFSC to address any issues there. Six paralegals are spread throughout the command to support the rest of the staff. CITF is a special case, with its own team of lawyers—one civilian, one active duty CID position, and four reservists.[60]

CID is also supported by a number of Reserve elements. There are three Reserve battalions and eighteen Reserve detachments which support CID, along with one National Guard battalion and six National Guard detachments. These units total 480 authorizations, of which approximately eighty percent have been filled, along with an additional eighty-two Drilling Individual Mobilized Augmentee agent positions. Though active for most of the reporting period, all CID National Guard units were inactivated on August 31, 2014. Reserve personnel have been a major asset to CID operations. The active and reserve components working together, an "AC/RC mix," provided benefits beyond raw manpower. Reservists brought many specialized skills to their CID missions, such as civilian police experience, arson investigation, or even accounting and

Fig. 3, CID Reserve Units[61]

Unit	[redacted]
595th MP Bn (CID)	Forest Park, GA
733rd MP Bn (CID)	[redacted]
159th MP Bn (CID)	Joint Base Lewis-McChord, WA
225th MP Det (CID)	Phoenix, AZ
[redacted]	[redacted]
380th MP Det (CID)	Oakland, CA
[redacted]	[redacted]
383rd MP Det (CID)	Lakeland, FL
[redacted]	[redacted]
366th MP Det (CID)	Worcester, MA
[redacted]	[redacted]
399th MP Det (CID)	St. Charles, MO
[redacted]	[redacted]
375th MP Det (CID)	Columbus, OH
[redacted]	[redacted]
220th MP Det (CID)	Scranton, PA
[redacted]	[redacted]
315th MP Det (CID)	Joint Base Lewis-McChord, WA

[60] LTC [redacted] interview, October 3, 2014, 1-2.

[61] "CID Reserve Unit Locations," U.S. Army Criminal Investigation Command, http://www.cid.army.mil/unitsreserve.html

financial forensics.[62]

Despite being a military organization, the civilian side of CID is crucial to is mission and continued operations. Civilians comprise over a third of the organization, filling vital roles in investigations, support, and the operation of the CRC and DFSC. A sizeable amount of growth within CID over the last few years has been among the civilians, rising from 746 authorizations in FY12 to 821 in FY13 and 879 in FY14.[64]

Fig. 4, CID National Guard Units[63]

Unit	Location
249th MP Bn (National Guard)	Austin, TX
1156th National Guard Det	Montgomery, AL
170th National Guard Det	Sacramento, CA
4175th National Guard Det	Fulton, MO
1149th National Guard Det	Abilene, TX
698th National Guard Det	Houston, TX
121st National Guard Det	Washington, D.C.

Though most SAs are military personnel, many of them are civilians. Their numbers have grown, reaching 315 in FY14, as opposed to only 250 in FY12. These civilian SAs handle specialized investigations, including with the units under the 701st. The MPFU is the main section with civilian agents. In FY14, the MPFU gained twenty-five authorizations, all but two of which were for agents, bringing their total authorizations up to 204. The CCIU is also largely civilian, with twenty-seven civilian SA authorizations in FY14, though it is scheduled to increase significantly over the next few years. Additional civilian SAs include two criminalistics agents, one FIU agent, and three polygraph examiners under the CRC. Furthermore, thirty Sexual Assault Investigators—eight of which were added in FY14—make up a relatively new force,

[62] "Command Brief," slides and accompanying information, U.S. Army Criminal Investigation Command, June 5, 2014, slide 10; COL [redacted] interview, September 18, 2014, 12-13.

[63] "Command Brief," slides and accompanying information, U.S. Army Criminal Investigation Command, June 5, 2014, slide 10.

[64] (b) (6), (b) (7)(C) "CID Current Force (FY12 Authorizations)," slide, USACIDC Manpower and Force Structure Division; (b) (6), (b) (7)(C) "CID Current Force (FY13 Authorizations)," slide, USACIDC Manpower and Force Structure Division; (b) (6), (b) (7)(C) "CID Current Force (FY14 Authorizations)," slide, USACIDC Manpower and Force Structure Division.

which has a great deal of experience within their area of focus.[65]

The Standards of Conduct Office (SOCO) was created in 2005. SOCO investigates allegations of agent misconduct, which it then turns over to the Judge Advocate staff if the allegations are substantiated. It acts as the internal review and policing body for CID, though it can only investigate with approval from the DCO. Despite the size of CID, SOCO is rather small. It began with a civilian director, a civilian agent, and two military agents. In the last few years, it had only growth slightly with a second civilian agent, though they have now lost one of their military agents and the other will likely be lost among the other Headquarters cuts. However SOCO has managed to fulfill its mission, aided by the continually low misconduct rates in CID; only five percent of agents on average are ever involved in misconduct investigations. The director of SOCO is (b) (6), (b) (7)(C).[66]

The bulk of civilian CID personnel are support and administrative staff. Seventy-four civilians, as of FY14, work at Headquarters in Quantico, fulfilling a number of functions. The Deputy Chief of Staff for Information Management (G-6) is responsible for the maintenance of all CID computer systems, as well as the purchasing and distribution of information technology to all CID personnel. The current G-6 is (b) (6), (b) (7)(C), who has held the position since 2007. She oversees a team of eleven civilian employees (and an additional thirty contractors), in turn coordinating with numerous IT positions at each of the CID subordinate units worldwide.[67]

In addition to the other Deputy Chiefs of Staff, there is also the Resource Management Division, led by the Comptroller (G-8). The G-8 is responsible for managing the budget and

---

[65] "Command Brief," slides and accompanying information, U.S. Army Criminal Investigation Command, June 5, 2014, slide 6; MG [redacted] interview, September 26, 2014, 10 ;Mr. (b) (6), (b) (7)(C), October 17, 2014, 11.

[66] CCWO [redacted] interview, October 24, 2014, 5-6; LTC [redacted] interview, October 3, 2014, 5.

[67] Ms. [redacted] interview, October 8, 2014, 1-3.

programming for CID. The current G-8 is (b) (6), (b) (7)(C) who entered the position in July of 2007. She oversees a team of eight civilians who work on three distinct areas: overall CID programming and budgeting, budgeting for CID Headquarters, and management analysis.[68] More on G-8 activities and CID budgeting will be discussed later in the chapter.

Furthermore, many of the sections under the G-1/4 are civilian run, including the Accreditations Division. (b) (6), (b) (7)(C) is the head of Accreditations and has been part of the division for almost thirty years. She oversees four other civilians who are responsible for badging and maintaining agent credentials. This includes monitoring changing policies as well as agent misconduct, tying in with the G-1/4, SOCO, and the Judge Advocate staff. The Accreditations Division also manages other smaller projects, such as the civilian clothing allowance provided to military SAs.[69]

Another division under the G-1/4 is Logistics, which is run by (b) (6), (b) (7)(C). She and her deputy oversee logistics positions across the command, managing the purchasing, disbursal, and maintenance of all equipment for CID. Additional responsibilities include tracking equipment, collecting and replacing older equipment, managing equipment storage, providing transportation for agents, and offering accountability training to personnel across the command. Logistics has been aided by a new tracking and management system program, the Global Combat Supply Support System. Unlike its predecessor, the Property Book Unit Supply Enhanced system (PBUSE), the new program "communicates and interfaces with the finance systems, with the warehouse supply systems…and with maintenance."[70]

---

[68] Ms. (b) (6), (b) (7)(C) October 17, 2014, 1-3.

[69] Ms. (b) (6), (b) (7)(C) September 18, 2014, 1-3; "Command Brief," slides and accompanying information, U.S. Army Criminal Investigation Command, June 5, 2014, slide 6.

[70] Ms. [redacted] interview, September 30, 2014, 1-5.

Beyond the Deputy Chiefs of Staff and their reporting sections, CID Headquarters is also home to the Public Affairs Office, which manages CID's public image, media relations, internal communication, and more. The Chief of Public Affairs, (b) (6), (b) (7)(C), acts as the CID spokesperson to the media and answers all media queries—which average well over a hundred each quarter. CID policy states that no agent or staff member will speak to the media or the public directly unless their statements are vetted and authorized by (b) (6), (b) (7)(C) and his staff also consult with their counterparts throughout the Army, the DoD, and the Department of Justice on when and how to release sensitive information. The PAO further reviews presentations made by members of CID (such as lab technicians) at conferences or other events. The PAO publishes the monthly command magazine, *The Shield*, as well as maintaining CID's website. Despite their breadth of responsibility, CID's PAO is much smaller than those of their counterparts, consisting of only three positions, including [redacted] With the sudden departure of one of their members in late 2014, the PAO has been left significantly understaffed.[71]

The Crime Records Center, also located within the Russell-Knox Building, is another source of civilian positions. The total number of authorizations for the CRC has held steady at fifty-four during the FY12 to FY14 period. Two warrant officers manage and assist with CRC operations along with forty-nine civilian positions that carry out its mission. One additional military position is also on loan to the CRC from the Headquarters staff. Rounding out the group are the aforementioned three CID polygraph examiners, who are provide quality control evaluations for all polygraphs performed by any examiner throughout the command.

The G-6 has assisted the CRC with one of its responsibilities: name checks. Due to the storing of all CID and MP investigatory files, the CRC runs certain background checks based on Secretary of the Army (SECARMY) directives. Many such directives were issued or expanded

[71] Mr. (b) (6), (b) (7)(C) April 6, 2015, 1-9.

during the reporting period. Two major areas of name checks involve childcare and promotions. Any member of the Army who comes into regular contact with children must be checked for past criminal activity. Candidates for promotions which require Senate approval are also given a similar screening. Both the depth and scope of checks has increased; originally only covering two categories (including detainee abuse), the directives expanded the screens to any infraction. Beyond the Senate-confirmable promotions, additional requests were made to screen any officer candidate, when originally only LTC and higher were required. These expansions were placed on top of CRC's existing responsibilities and compounded by directives to screen all new personnel and an increase in background check requests from the DoD and the Office of Personnel Management. Traditionally, the turnaround time for a name check was about forty-five days. With G-6 help in accessing electronic databases, the CRC was able to decrease the delay to about a week. However, with the recent flood of name checks which multiplied over the course of 2014, the CRC cannot maintain their turnaround time. They are understaffed to manage the rapid increase in volume, which totaled almost 320,000 name checks by the end of 2014.

The G-6 has also worked with the CRC to automate a number of its processes and digitize most of the information coming in from the field to increase efficiency and productivity. Previously, upon closing a case, agents would send the Report of Investigation (ROI) and all accompanying materials to the CRC, which would then store the physical copies and eventually scan them. Now, the G-6 has provided scanners to the offices of every CID unit, allowing them to make a digital copy of these exhibits and then send them to the CRC electronically. Though a significant investment, digitizing will save a great deal of time and money. Mailing an ROI costs about ten dollars. Though seemingly inexpensive, the CRC receives over 12,000 ROIs annually, which adds up to substantial savings. It has taken time to gain traction, but the digitization effort

is ongoing. Furthermore, CRC is responsible for storing fingerprints of individuals involved with CID cases. Until recently, CID was still using inked fingerprints as opposed to digital. They are now using digital scanners, as discussed below.[72]

Such activities tie the CRC with the DFSC, which is another major civilian element of CID. The DFSC has experienced significant growth and is scheduled to continue to expand in the coming years. The USACIL section, the primary forensics section, gained five authorizations from FY12 to FY13/14, reaching 167 positions. With the reorganization into the DFSC, the Army approved 152 additional requirements for the Office of the Chief Scientist (OCS) and the Forensic Exploitation Directorate (FXD) during the FY10-14 period. USACIL, OCS, FXD, and the DFSC support staff totaled around 320 civilian employees, with 351 requirements slated for FY15. The expeditionary capability, especially the FXTs, was built up during active operations in the Middle East. The ability to gather and use evidence in theater was a crucial ability and was given priority for funding. With active operations largely done and the Army cutting all extraneous spending, funding for this capability is drying up. With the manpower built up over the years, CID is attempting to preserve the FXD and their FXTs, though cuts are expected.[73]

In addition to their manpower resources, CID also has a great deal of technology and equipment at their disposal. The DFSC uses a number of state of the art machines to process physical evidence, such as fingerprints. Until 2014, CID was using fingerprints taken with ink, which would then be scanned by the CRC and sent out to an FBI fingerprint database, the Criminal Justice Information Service (CJIS). The inking process had several issues. It was

---

[72] Ms [redacted] interview, March 30, 2015, 1-8; "Command Brief," slides and accompanying information, U.S. Army Criminal Investigation Command, June 5, 2014, slide 6; Ms. [redacted] interview, October 8, 2014, 3; Mr. [redacted], October 15, 2014, 5-6; [redacted], "ROIs go digital: Saves time, saves money," *The Shield*, November 2014.

[73] "Command Brief," slides and accompanying information, U.S. Army Criminal Investigation Command, June 5, 2014, slide 6; Mr [redacted] interview, October 17, 2014, 3; Mr. [redacted], October 15, 2014, 9.

inefficient, as it required multiple steps to reach CJIS. It took a long time for the prints to be put into the database, both by the CRC and by CJIS. This delay had the added problem that if an issue with the prints was discovered—if they were smudged, for example, which was common with inked prints—then it was difficult or potentially impossible to reprint the individual, as the problem could be discovered weeks, months, or more after the prints were first taken. If the original inking had occurred in theater six months prior, then the odds of finding the individual again were slim. Due to such problems, other MCIOs had previously switched to electronic fingerprint scanners. Backed by (b) (6), (b) (7)(C), CID made the transition in 2014, buying over $3 million of fingerprint scanning equipment. The new technology is more efficient, immediately making a digital copy at the investigative offices and uploading to the CRC. It is also more thorough, capturing all ten fingers, palm prints, and the "karate chop" (the side of the palms).

(b) (6), (b) (7)(C) is also trying to make photo recognition part of the booking processes in addition to the fingerprinting. When a suspect has their hands scanned, they would also have their picture taken and run through a database of known and unknown criminals. Another emerging forensic technique is the use of rapid DNA testing. As opposed to traditional DNA tests, this technique takes only about an hour to analyze. The disadvantage is that this technique is only about ninety-two percent accurate, lower than most state and federal guidelines. Ultimately, CID's goal is to have a complete booking station which would check a suspect's fingerprints, face, and DNA in a short amount of time. However, the realization of this concept is still a few years away.[74]

Other forensic equipment can be taken by Special Agents (FSO and FSTs) directly into the field. One example is the Faros machine, a scanner with captures a three-dimensional rendering of a room or area, which can be used for crime scene reconstruction. Another important resource is Cellebrite equipment. These machines can extract and copy data from

[74] Mr. (b) (6), (b) (7)(C) October 15, 2014, 5-6.

electronic devices, such as smartphones, providing data and digital evidence to investigators. This evidence can in turn be used to build a case (via call history, text messages, etc.) or be further analyzed by Digital Forensic Examiners (DFEs).[75]

For CID's own electronics needs, the G-6 purchases all IT technology and distributes it to CID personnel. These resources—such as computers and phones—are largely pre-chosen by the Army. They have standard items supplied via coordinated contracts with private companies, such as Microsoft. As such, the G-6 does not have to 'shop around' for equipment, just request the basic type of equipment and the Army will provide it. In addition to hardware, this is primarily the case for as well, such as with Adobe licenses. As far as hardware, the Army's preferred phone is Blackberry, though there is an iPhone pilot project currently underway.[76]

Tablets are a technological resource that is new to CID, which originated in 3rd MP Group. With initial success at 3rd MP Group, they sent the idea to the CG for approval. MG [redacted] approved tablets for the entire command in 2014. His rationale was: "when I go to a crime scene, why am I taking pictures with a camera and taking notes? Why don't I have a tablet in which I take pictures of the crime scene…? I can take statements, I can audio record them. I can do all this kind of stuff on a tablet. And then I hit the send button and it automatically loads up into our database." The tablets should increase efficiency and effectiveness of CID investigators, as well as permit CID personnel to investigate from a distance. A forensic expert (or a superior officer) could connect to an investigator's tablet, analyzing its contents and viewing the crime scene via the tablet's camera, regardless of distance. The tablets' acquisition is also an example of inter-agency cooperation. Air Force OSI had previously tested one of the two

[75] CSM [redacted] interview, October 15, 2014, 4-6; Ms. [redacted] interview, September 30, 2014, 1-3.

[76] Ms. [redacted] interview, October 8, 2014, 7.

tablet models CID was considering and cautioned them against it, leading CID to choose the better of the two models.[77]

The CCIU has also developed a new digital tool to help in their cyber investigations. The Rapid Extraction and Analysis Program, or REAP, is a program built by CCIU's own research and development section as a diagnostic and investigative tool. If an Army computer is believed to be compromised, CCIU can provide this program to the network administrator and they will upload it to the computer. REAP then automatically runs a number of tests and returns a digital "snapshot" of the state of the suspected computer. From there, CCIU specialists can analyze the results and determine if the system has been compromised. This procedure allows the CCIU to immediately begin its investigation wherever the suspicious activity occurred, even if their agents are geographically far away.[78]

Another major update in equipment was CID credentials. In the spring of 2012, all military and civilian agents, as well as reserve agents and select staff positions, received brand new credentials. Since their inception in the 1970s, CID credentials had remained largely unchanged, created on a typewriter and assembled by hand. The new credentials are produced by an automated system which includes a number of new features, including security holograms and a digital photograph of each credential holder. The new system produces credentials much more efficiently and can easily create new credentials in the case of loss, damage, or change in personal information (such as change of name). The process of swapping out the old credentials for the new ones lasted throughout 2012 into 2013. As of 2014, all required personnel have

[77] MG (b) (6), (b) (7)(C) interview, September 26, 2014, 22; COL (b) (6), (b) (7)(C) interview, December 15, 2014, 3; COL (b) (6), (b) (7)(C), September 18, 2014, 15.

[78] Mr. (b) (6), (b) (7)(C), interview with (b) (6), (b) (7)(C) and Dr. (b) (6), (b) (7)(C), Quantico, VA, April 14, 2015, 7-8.

received their new credentials, though a few remaining old credentials—particularly among reserve agents—still need to be returned.[79]

Equipping a force such as CID is not an easy task. It is not as straightforward as it would seem, due to the nature of CID's mission. CSM (b) (6), (b) (7)(C) explained that as a law enforcement agency, an MCIO, and a deployable force, CID has specialized needs for their equipment. Even a seemingly simple item, such as a flashlight, takes careful consideration, "because the flashlight that we give a CID agent has to go from the practical policing back in garrison all the way to a tactical environment." Rather than a simple white light, a flashlight would also need "ambient lighting to try to find latent prints or footprints or evidence on a crime scene, but it also has to have...tactical lighting so when you're in a tactical situation...you can't be picked up as you're reading your maps in red light, blue light, or green light. It also has to have infrared so you can see it with your night vision goggles." CID is unique in the demands it has on its agents and their equipment while "regular law enforcement doesn't have to have all those requirements."[80]

Such considerations are also taken into account for more serious equipment, such as firearms and body armor. The standard issue sidearm for CID agents is the M11 SIG Sauer. PSB agents and agents deployed on combat operations carry M4 rifles, a more compact version of the M16. They formerly used H&K MP5 submachine guns for this purpose, but began phasing that model out in 2013.[81] Another significant change was the addition of concealable body vests distributed to CID agents. The vests were previously in use, but were funded individually by CID itself. Within the last year, the purchasing of the vests transferred to the general Army budget,

---

[79] Ms. (b) (6), (b) (7)(C), September 18, 2014, 1-2; COL (b) (6), (b) (7)(C) interview, October 8, 2014, 2; (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) "New CID credentials release to the field nearly complete," *The Shield*, October 2012.

[80] CSM (b) (6), (b) (7)(C) interview, October 15, 2014, 5-7.

[81] SA (b) (6), (b) (7)(C) "Take the Shot," *The Shield*, May 2013; (b) (6), (b) (7)(C), "Training with the Army Marksmanship Unit," *The Shield*, December 2013; CPT (b) (6), (b) (7)(C), "3rd MP Group trains with the Army Marksmanship Unit," *The Shield*, August 2014.

allowing for more vests to be acquired. The ultimate goal is to have each agent fully equipped upon graduating from their CID training, rather than placing that responsibility on their first assignment.[82]

Funding CID as an organization is also not easy. As examined in the last chapter, managing the CID budget has been a struggle during 2013 and 2014, contending with Continuing Resolutions, Sequestration, and overall disruption in normal budgeting processes. The end of active operations overseas has also slashed CID's finances dramatically. Its total budget in FY13 was $300 million, falling to $200.9 million in FY14. This is a drastic change, though it should be noted that the shortfall is entirely in OCO funds, falling in parallel with the Army withdrawal from the Middle East. CID's base budget grew during the period, from $131.5 million in FY13 to $142.4 million in FY14. Nevertheless, total finances have taken a heavy hit, inhibiting growth and expansion that had previously been on the books.[83]

CID as an organization grew in overall size during the reporting period. Its footprint grew almost 400 authorizations over the course of two FYs, as presented at the start of the chapter.

Fig. 5, CID Budget, FY13, & FY14[84]

	Base Budget	Base as % of Total	OCO Funds	OCO as % of Total	Total Budget
FY13	$131.5 million	43.83%	$168.5 million	56.17%	$300 million
FY14	$142.4 million	70.88%	$58.5 million	29.12%	$200.9 million

[82] Ms. [redacted] interview, September 30, 2014, 1-3.

[83] Ms. [redacted] interview, October 17, 2014, 12-13.

[84] Ms. [redacted] interview, October 17, 2014, 12-13.

With its continuously evolving mission, CID leveraged additional resources to promote its expansion. The primary growth in FY13 was among special agents, both civilian and military. General military SA authorizations grew seventy-three spaces, intended to combat installation crime. This helped to balance out CID agent numbers at camps, posts, and stations across the country, as large amounts of SAs had deployed overseas. Of the seventy-three, forty-six were dispatched to 3rd MP Group and the remaining twenty-seven went to 6th MP Group. Technical and analyst positions increased as well, with ten eGuardian and twenty-seven criminal intelligence (crim-intel) authorizations. Another major area of growth is in the MPFU, which has been approved to grow by 173 authorizations over the next several years. The MPFU added thirty-three authorizations in FY13, thirty of which were civilian SAs paired with three support positions.

The restructuring of CID in alignment with Army downsizing was able to conserve authorizations and cut in areas that were no longer needed. As a result of the deactivation of the 202nd MP Group and the 1002nd MP Bn in Europe, twenty-seven authorizations were transferred to the PSB and thirty-one TDA authorizations were able to be eliminated. While technically a loss, these authorizations were legacy requirements from the deactivated units and were now unnecessary. Their elimination limited the number of authorizations that CID had to compete for in the 2013 TAA. The only true losses were eight mechanic authorizations cut to meet new requirements from the U.S. Army Training and Doctrine Command (TRADOC).[85]

Growth continued steadily in FY14. MPFU added another twenty-five authorizations—twenty-three SAs and two support staff—in line with its ongoing concept plan. Sexual assault sections also received a boost, gaining eight Sexual Assault Investigators, three military Sexual

[85] Mr. [redacted] interview, October 3, 2014, 2-3; [redacted] "Current Manpower and Force Structure Actions," April 24, 2013, 1-3.

Assault Response Coordinators, and three civilian Victim Advocates. These latter two positions were spread out among the Groups, one of each type at 3rd MP Group, 6th MP Group, and the 701st MP Group. Twenty-two more crim-intel positions were added, though they are slotted to be reinvested in the DFSC, which will be discussed below.

The biggest acquisition in FY14 was the full authorization of Drug Suppression Teams throughout the command. Each of CID's thirty-two detachments received a team of five 31B MP troops to run drug suppression missions. Each MTOE Battalion also received a warrant officer to manage the DSTs. These additions, totaling 166 positions—160 MPs and six warrant officers—has facilitated the transition to twenty-six person detachments and three-agent teams as described in the last chapter. The consolidation of these MPs directly under CID control was not only an administrative aid; it also helped in terms of finances and manpower. Before the transition, the MPs used in DSTs were pulled from a combat support company. When the company was dissolved and split into the five-soldier groups disbursed to the detachments, the remaining authorizations were put towards incoming manpower cuts and shoring up areas of CID growth.[86]

Even in the midst of the Army drawdown, CID has still planned to grow, into FY15 and beyond. In the years leading up to the reporting period, many areas of growth had been scheduled and approved for FY16 through FY19. The MPFU was set to continue on its concept plan, picking up another fifty-one authorizations in the coming years, with a forty-eight/three SA/support staff split. Another eight Sexual Assault Investigators and three Victim Advocates are also set to be added. The DFSC, another major area of growth, has eighty-nine authorizations scheduled, primarily supporting its expeditionary forensics capabilities. However, funding all of these positions has been difficult. CID has had to fight and compensate to continue their growth.

[86] Mr [redacted] interview, October 3, 2014, 3; [redacted] "Current Manpower and Force Structure Actions," January 17, 2014, 1-3; [redacted] "Current Manpower and Force Structure Actions," July 31, 2014, 1-4.

For the eighty-nine DFSC spots, they had to invest the aforementioned twenty-two crim-intel positions. Only by paying for those positions internally would the Army fund the remaining sixty-seven.

Despite this planned growth, CID is also facing large cuts. Between Army downsizing, DoD mandates, and the aftereffects of Sequestration, CID's growth will be extremely limited, both for the Operating Force (OF)—the active and deploying side of the Army and CID—and the Generating Force (GF)—the support side of the Army and CID. There has been some decrease in how steep the cuts will be. With the reorganization of the MPs and the shift of eighty-eight other military authorizations to the OF, CID has negated most cuts to the GF. Nevertheless, the final status of the OF and GF remains uncertain.

As discussed in Chapter 2, CID is facing a 146-position cut during the FY16-19 period. Eight of the positions are military, specifically the Headquarters staff. An additional sixteen civilian staff from Headquarters are also set to be cut. Seventy-three "core operations" civilian authorizations will be reduced, including fifty-four positions at the DFSC. The MPFU will lose forty-five agents and the crim-intel staff will lose four positions.

The combination of growth and cuts are slated to work in tandem. The growth is ambitious, although the cuts are also quite high. As a result, they essentially cancel each other out. The planned cuts negate ninety-one percent of the scheduled civilian growth over the next several years. The Headquarters cuts, proportionally, are the most drastic and there is no planned growth that counteracts the cuts, nor has the Headquarters significantly grown since the 1990s. The original fifty-one MPFU positions will be whittled down to six, only three of which are agents. The DFSC, originally meant to receive eighty-nine new authorizations, will be left with thirty-five—only enough for a single FXT, when three were planned. Overall, CID will only net

an increase of thirteen civilian authorizations from a scheduled increase of 151, and the losses and gains will be uneven.

However, CID is taking steps to counteract these steep cuts and continue expanding in the face of these reductions. COL [redacted] as DCO, introduced a Directed Military Overstrength (DMO) for CID Headquarters to ease the imminent cuts there. The DMO will add ten military positions for two years, with the hope that these requirements may eventually be made permanent. The new positions include a major and two captains to assist the G-2/3 and other officers to support the G-1/4 and the Staff Judge Advocate. There are three primary concept plans which have been submitted to Army leadership for approval. These plans outline additional growth to allow CID to meet the demands of continuing and emerging missions, especially by their specialized units. One concept plan is requesting thirteen requirements for the PSB to solidify its intelligence capabilities, which were originally set in place by a DMO in 2012. The second plan doubles the size of the CCIU, adding an additional thirty-two requirements. Twenty of these requirements would be military while the remaining twelve would be civilian—ten of which CID has offered to pay for in-house. The third concept plan finalizes the realignment of the CITF under the 701st, authorizing thirty military, twenty-six civilian, and twenty-four contractor positions.[87]

CID, though a relatively small part of the Army, is a robust organization with significant manpower and technological resources at its disposal. Though future cuts may threaten the growth it has experienced in 2013 and 2014, CID has continued to carry out its many missions. Details of its operations and activities will be discussed in Chapter 4.

---

[87] Mr. [redacted] interview, October 3, 2014, 3-6; COL [redacted] interview, October 15, 2014, 2-6; Mr. [redacted] interview, April 14, 2015, 1-3; [redacted] "Current Manpower and Force Structure Actions," January 17, 2014, 1-3; [redacted], "Current Manpower and Force Structure Actions," July 31, 2014, 1-4.

Chapter 4: Operations

"You don't really appreciate all the CID Command does until you have had the job," stated MG [redacted] about the breadth of CID's mission. "And all the intricacies that it touches, and all the capabilities that it brings to bear, is quite incredible."[88] CID operations encompass felony investigations, but also include diverse areas such as protective services, digital and financial crime, forensic testing, and supporting active forces in-theater. This chapter will discuss CID's ongoing mission during 2013 and 2014, following the investigations at home, the activities of its specialized units, DFSC operations, and CID deployments overseas.

In FY13, CID launched 12,728 Reports of Investigation (ROI) and 9,559 non-ROI investigative sequence actions, with a total 97.2 percent solve rate. In the first half of FY14, CID created 4,737 new ROIs and over 4,084 non-ROI investigative sequence actions, with a total 97 percent solve rate. This solve rate is significantly above the national averages for law enforcement organizations. For violent crimes, the national average solve rate was 47.7 percent in FY13 and 46.8 percent in FY14. For property crimes, the national average solve rate was 18.6 percent in FY 13 and 19 percent in FY14. In addition to its high solve rate, CID was also instrumental in the recovery a massive amount of money in FY13 and FY14, stemming from various frauds and false claims. The total amount by mid-2014 reached over $114,000,000, much of it returned to the U.S. Treasury.[89]

CID investigates all manner of crimes, though perhaps the most obvious area is death investigations. One such investigation garnered extensive media attention: the Ft. Hood shooting

[88] MG [redacted] interview, September 26, 2014, 1.

[89] "DAHSUM, FY 2013," 6; "2014 Spring Semi-Annual Report to Congress," 1-2.

Fig. 6, CID Solve Rates in Percentages, FY13 & FY14[90]

	Drug Crimes	Persons Crimes	Economic Fraud	Violent Deaths	Sexual Assault	Property Crimes	Misc. Crimes	Overall Average
FY13	99.6	94	95	94	87	64	100	97.2
FY14	99.2	93.7	96.7	86.1	86.1	67.6	87.9	97

on April 2, 2014. The perpetrator, SPC Ivan Lopez, opened fire at several sites across Ft. Hood, TX. He killed three soldiers and wounded sixteen other people before finally turning the gun on himself. Lopez had argued with several of the people he attacked that morning regarding a denied request for leave. The exact motive for the shooting is unknown, though Lopez had been struggling with mental health issues. The attack was an eerie reminder of the 2009 shooting at Ft. Hood carried out by MAJ Nidal Hasan, who killed thirteen people and wounded over thirty others. Hasan was convicted on August 23, 2013, and sentenced to death.

CID was a crucial part of the 2014 case, just as it was in 2009. CID agents were among the first on the scene on April 2 and were a central force in the establishing of crime scenes and the ensuing investigation. They coordinated with MPs, FBI agents, Texas Rangers and local police departments to secure the area, process witnesses, take statements, and analyze evidence. Through the cooperation of CID with these other organizations, the truth of the shooting, which was at first highly fragmented, became a clearer picture. The Chief of CID Public Affairs was dispatched to the scene and managed the Army's response to the media, informing the public about the facts of the shooting.[91]

[90] "DAHSUM, FY 2013," 1; "2014 Spring Semi-Annual Report to Congress," 6. In this chart, "Sexual Assault" includes only violent sex crimes. The FY14 solve rate covers until February 2014.

Ft. Hood was just one of a number of death investigations handled by CID—and not all deaths are at the hands of someone else. CID also investigates suicides under their jurisdiction and assists OPMG as part of the Suicide Task Force. They helped in the production of the Red and Gold Books, both in-depth studies on suicides in the Army. However, under the direction of MG[redacted] CID and OPMG shifted its main focus away from suicides towards other areas.[92]

One new area was sexual assault. The Chief of Staff of the Army (CSA), GEN Raymond T. Odierno, stated that battling sexual assault is a top priority: "Our profession is built on the bedrock of trust; sexual assault and sexual harassment betray that trust."[93] CID investigates all accusations of sexual assault involving Army personnel, including unwanted sexual contact. They make great attempts to prevent sexual assault and stop it in its earliest forms, to prevent it from escalating to rape and violence. This effort includes crim-intel analysis and forensics, as the technological capabilities of CID have expanded in this regard. Increased staff and new technology at USACIL lowered turnaround times on DNA and other physical evidence from sexual assaults, aided by new sexual assault evidence collection kits. These kits, first introduced in 2012 and distributed through the command during the reporting period, are a major update of the previous model. They are standardized and better organized, contain more collection materials, and can be stored at room temperature without samples degrading.

All of these endeavors come together as part of CID's professionalism; their handling of such cases is very thorough and methodical. New investigative techniques have also helped to better solve these crimes. [redacted], Chief of the Family Advocacy Law Enforcement

---

[91] "Fort Hood Shooting," *The Shield*, May 2014; SA[redacted] MAJ [redacted] "Success in Chaos: An inside look at the recent active shooter at Fort Hood," *The Shield*, July 2014; "DAHSUM, FY 2013," 24; [redacted] interview, April 6, 2015, 4-5,

[92] MG[redacted] interview, September 26, 2014, 3-5; CCWO [redacted] interview, September 30, 2014, 2.

[93] GEN Raymond T. Odierno, "CSA Sends: Sexual Assault and Sexual Harassment," *The Shield*, June 2013.

Training Division at USAMPS, is a renowned expert on sexual assault crimes and a major force behind CID success. A retired CID agent himself, Strand established the DoD Special Victims Unit Course and pioneered the Forensic Experiential Trauma Interview (FETI). This is a revolutionary approach to victim interviews that "'draws on the best practices of child forensic interviews, critical incident stress management, and motivational interview techniques...into a simple, three-pronged approach; unlocking the trauma experience in a way that can be better understood.'" Victims of traumatic events do not usually have clear recollections of the basic information that law enforcement officials are trained to glean from interviews—the "who, what, and where" of a crime. The FETI technique helps draw out the necessary information from victims gently but effectively.

Strand originally developed FETI in the wake of the 2009 Ft. Hood shooting while interviewing survivors. He has since begun teaching the technique at USAMPS and the Federal Law Enforcement Training Accreditation Board fully certified the class on April 25, 2013. The DoD has funded the class through FY17 with 400 seats annually. Around 1,400 military investigators and prosecutors—from all branches—have participated in FETI training, and it has spread into other sectors as well. More than 150 organizations from the local to international levels have taken part in FETI courses, including thousands of individual students such as victim advocates and health care professionals. FETI, along with other related training courses run by Strand, have helped bolster the effectiveness of CID and other law enforcement agencies as they pursue sexual assault investigations.[94]

---

[94] Quote from (b) (6), (b) (7)(C) in (b) (6), (b) (7)(C) "Game Changer: The FETI Technique," *The Shield*, August 2013; additional information from COL (b) (6), (b) (7)(C), September 18, 2014, 1, 10-11; MG (b) (6), (b) (7)(C) interview, September 26, 2014, 21-28; (b) (6), (b) (7)(C), "New sexual assault evidence collection kit," *The Shield*, August 2012; (b) (6), (b) (7)(C) "Innovator in combating sexual assault receives national recognition," *The Shield*, February 2012; "Game Changer: The FETI Technique," *The Shield*, August 2013; (b) (6), (b) (7)(C) "Former CID Agent develops interview method to help unlock memories, reduce revictimization," *The Shield*, September 2014.

Children are another victim pool for sexual assaults and abuse. SA(b) (6), (b) (7)(C) has introduced a new initiative consisting of seminars at high schools which discuss this painful subject. In addition to educating young adults about the dangers of sexual assault and how prevalent it can be, these "Break the Chains" events have encouraged victims to come forward and allowed them to get the help they need. While the goal of the program was not to seek convictions, there have been many as a result of information gained after the seminars. [redacted] is hoping to expand the program, creating new seminars to be used across the command, at middle schools as well as high schools, and an adult course to reach older victims.[95]

Beyond physical crimes, CID investigates other felonies, particularly by the specialized units of the 701st MP Group. The MPFU has continued its mission investigating contingency operations corruption and fraud. During the reporting period, the MPFU maintained four forward-operating offices in Kuwait and Afghanistan. These offices investigated contractual fraud in support of Operations Enduring Freedom and New Dawn. This unit launched hundreds of ROIs during the reporting period, with 321 ROIs in the span of October 2013 to March 2014 alone. These in turn have led to millions of dollars' worth of recoveries; each MPFU agent returns approximately $2 million dollars to the Army annually. Near the start of the reporting period, at the end of FY12, the MPFU's overall recoveries since its inception totaled more than $2.2 billion. As one of the rare units in the Army to recoup its budget—and then return a profit to the government—the MPFU expanded during the reporting period. As discussed in the previous chapter, they gained twenty-five authorizations in FY14 and were slated to expand even more, though Sequestration and budgetary constraints will limit that growth in the future.

---

[95] (b) (6), (b) (7)(C), "Breaking Chains," *The Shield*, February 2014.

Fig. 7, MPFU Recoveries, 2013 & 2014[96]

	2013	2014
MPFU Recoveries	$169 million	$945 million

Nevertheless, the MPFU itself expanded, as did its mission, with agents deploying to the Middle East to investigate OCO contracts firsthand. This move was a success, rooting out a great deal of fraud in-theater and returning more funds to the government and the Army. One such case, which came to fruition in 2014, proved to be the largest recovery in the history of the unit. The successful investigation by the MPFU of a dining contractor which was defrauding the government resulted in a massive settlement: $389 million dollars. That amount exceeds what the unit often recovers in an entire year. 2014 marked a record for the most financial recoveries by the unit as well, even without the food provider case. Still, the amount of money recovered by the MPFU, though considerable, varies greatly from year to year as their cases can take several years—even five to seven years—to reach completion. It can take a long time to see any gains from a case and in some instances there is no financial return at all. To continue pursuing such cases, MPFU training also underwent some changes. The unit worked with the Defense Acquisition University to create a new class particularly targeted for investigators. They have also added more Digital Forensic Examiners into the unit to pursue the digital aspects of fraud.[97]

The CCIU, another specialized unit, investigates digital crimes, intrusions into Army networks, and insider misuse of Army computer systems. Digital crime has grown exponentially

[96] Mr. [redacted] interview, April 14, 2015, 5-6.

[97] Mr. [redacted] interview, April 14, 2015, 1-7; Mr. [redacted] interview, October 17, 2014, 10-11; COL [redacted] interview, October 15, 2014, 1-2; "DAHSUM, FY 2013," 8; "2014 Spring Semi-Annual Report to Congress," 3-4. [redacted] "MPFU racks up returns," *The Shield*, March 2013.

in the last few years and continues to do so. Much like the MPFU, the CCIU expanded to meet these growing threats, opening a new Pacific office at Joint Base Pearl Harbor-Hickam in Hawaii. This new site was activated on July 31, 2013, and reached Initial Operating Capability two days later. Several other new offices around the world are slated to open in the next several years, increasing CCIU's global footprint. This growth is in conjunction with the twelve civilian and twenty military positions that are planned to be added to the CCIU, as discussed in Chapter 3. The Pacific office is jointly located with the Defense Information Systems Agency Pacific Cyber Center. Additionally, the CCIU worked extensively with the U.S. Army Cyber Command (ARCYBER), with its agents and analysts seeking out intrusions and performing crime prevention surveys. CCIU conducts assessments of various Army and DoD sites, examining their classified and unclassified networks to look for potential weaknesses and exploits. After these annual evaluations, each site has thirty days to fix any issues the CCIU discovers. During the reporting period, following the last CCIU set of examinations, no assessed locations experienced any network compromises. This has created a $149.1 million cost avoidance to the Army and the government since FY13. The CCIU also focuses on internal threats, leading cyber espionage investigations, monitoring unauthorized access, and testing the vulnerability of CID networks.

In the course of their emerging mission, CCIU has tackled a number of high-profile cases. The unit led the joint investigating of the PFC Manning case, "the largest compromise of classified material in U.S. Army history." PFC Manning, an analyst in Iraq, used Army credentials to access and gather massive amount of classified documents from government networks in 2009. Manning then proceeded to leak the information to the website WikiLeaks, which in turn broadcast the materials to the public. Manning was tried in 2013 and found guilty of numerous charges including espionage, and is currently imprisoned at Ft. Leavenworth U.S.

Disciplinary Barracks serving a thirty-five year sentence. Other prominent cases include the charging of a British hacker with attacking Army networks and the indictment (and later conviction) of nine individuals involved in a fraudulent tax refund ring in the Ft. Benning area which stole $20 million from the government.[98] In May 2013, the CCIU took on a new responsibility safeguarding the digital personas of important individuals. They established a new task force, the Cyber Assurance and Investigations Team (CAIT), in order to protect the digital records of the Secretary of Defense and other key DoD personnel. Up to that point, the President and Vice President were the only government officials to have digital protection, which is provided by the Secret Service. CAIT now prevents unwanted access to personal information and records (e.g. financial, medical, and educational) by third parties, as well as monitors threats directed towards these people that use a digital medium, such as a blog.[99]

The PSB handles the physical protection of these high-risk personnel (HRPs). Though not an investigative unit, the PSB's mission is nevertheless a critical one. The PSB provides "continuous worldwide executive protection from assassination, kidnapping, injury and embarrassment for designated senior high-risk personnel of the DoD, the Joint Chiefs of Staff and Army, and for their foreign counterparts during official visits to the United States." Working in tandem with the CCIU, the PSB managed the Digital Persona and Personal Identifiable Information (PII) protection program for HRPs. They conducted several hundred personal

[98] Mr. [redacted] interview, April 13, 2015, 4-12; (b) (6), (b) (7)(C), editor, "CCIU Overview," slides, U.S. Army Criminal Investigation Command Computer Crime Investigative Unit, updated 2015; [redacted]. (b) (6), (b) (7)(C) comp, "Computer Crime Investigative Unit (CCIU)," U.S. Army Criminal Investigation Command, updated 2015; see also "Alleged Hacker Indicted In New Jersey For Data Breach Conspiracy Targeting Government Agency Networks," Department of Justice Press Release, October 28, 2013; "Twenty Million Dollar Stolen Identity Refund Fraud Ring Indicted," Department of Justice Press Release, May 22, 2014; "Nine Defendants Plead Guilty in $20 Million Stolen Identity Refund Fraud Ring," Department of Justice Press Release, April 1, 2015.

[99] MG [redacted] interview, September 26, 2014, 10; COL [redacted] interview, October 15, 2014, 2-3; Mr. (b) (6), (b) (7)(C) interview, April 14, 2015, 1-12; Ms. [redacted] interview, October 8, 2014, 6; "DAHSUM, FY 2013," 7-8; "2014 Spring Semi-Annual Report to Congress," 3; CCWO (b) (6), (b) (7)(C), "Chief Speak," *The Shield*, May 2013; (b) (6), (b) (7)(C), "CCIU Establishes Pacific Office," *The Shield*, October 2013; (b) (6), (b) (7)(C) "CCIU Establish Task Force: Protects Online Persona of SEC DEF, Others," *The Shield*, April 2014.

security missions for HRPs during the reporting period, both domestically and in deployed environments. The PSB has also carried out dozens of foreign minister security missions, such as guarding GEN COL Saken Zhasuzakov, First Deputy Minister of Defense of Kazakhstan, on his 2013 visit to FORSCOM. The PSB, in size and scope of its mission, continues to grow. In addition to key DoD and Army staff, the PSB has also added the Chief of the National Guard Bureau to its roster of HRPs. The PSB manages and trains the personal security details for the Combatant Commanders of SOUTHCOM and USFK. In accordance with DoD directives, these details will move fully under CID, which is a Protection Providing Organization (PPO). The SOUTHCOM detail of one 311A warrant officer and twenty-two 31D NCOs will come under 3rd MP Group in FY15, and the USFK detail of one 311A warrant officer and seventeen 31D NCOs will come under 6th MP Group in FY16.

The PSB also expanded its intelligence capabilities with the creation of a 24-hour watch and support team. Driven by COL [redacted] the intelligence section of the PSB grew from only three civilian positions to seventeen, including military intelligence specialists and an MP Captain to oversee the group. In addition to its around the clock support ability, PSB analysts also carried out security vulnerability assessments and threat assessments on all travel missions for HRPs, using a risk analysis program that integrated terrorist and criminal threat data. Personal security is a very manpower-intensive mission. In response the PSB was able to increase its numbers, gaining several positions with the deactivation of the 202nd MP Group as well as the addition of 31B combat support MPs, as discussed in Chapter 3.[100]

[100] Quote from ; "DAHSUM, FY 2013," 7; information from COL [redacted] interview, October 15, 2014, 2-4; CCWO [redacted] interview, October 24, 2014, 8; "DAHSUM, FY 2013," 6-7; "2014 Spring Semi-Annual Report to Congress," 2-3; Protective Services Battalion, "PSB Mission: Kazakhstan," *The Shield*, March 2013; "Current Manpower and Force Structure Actions," July 31, 2014, 3.

Also mentioned in the last chapter, MPs were added to Drug Suppression Teams (DSTs) to meet the demands of that emerging mission. The dedicated MP positions have helped cement the DSTs and allowed them to pursue more investigations. Members of these teams go through extensive training and practice exercises; these simulations include coordinating with canine units and tactical response teams. DST operations also often have an undercover component, which makes the training, especially the joint preparations with tactical teams, all the more important. The DST of the Washington Battalion has been especially effective, conducting a large number of "busts" in 2013 and 2014.[101]

The FIU, another part of the 701st, handles sensitive and covert operations for CID. Due to the nature of their investigations—and the classified materials they handle—not much information is released about the FIU. The cases investigated by the FIU can range from investigations of senior Army leaders to fraud investigations of specialized Army programs, such as research and development. During the reporting period, the FIU gained a civilian MPFU investigator to help with such cases, as well as a number of civilian positions to help ensure continuity in the unit.[102]

Supporting all of these specialized units and overall operations is the Command Intelligence Operations Center (CIOC) based out of CID Headquarters. This team analyzes and distributes intelligence to field teams across CID. The CIOC helped the Army expand its eGuardian program, a system allowing the rapid sharing of information on suspected terrorist activities with the DoD, FBI, and other law enforcement agencies of all levels. They managed

---

[101] "The Art of the Bust," *The Shield*, February 2013; [redacted], "Joint CID, MP Exercise Showcase Special Skills," *The Shield*, November 2014; MG [redacted] interview, September 26, 2014, 5-6; COL [redacted] interview, December 15, 2014, 5.

[102] COL [redacted] interview, October 15, 2014, 4; [redacted], "Secret Soldiers: CID Field Investigative Unit," *The Shield*, April 2013.

almost 500 eGuardian accounts and helped to expand the FBI eGuardian Suspicious Activity Report system by imputing Army data. The CIOC also has two specialized analysts, one dedicated to intelligence related to domestic extremism and gang activities and another dedicated to drug abuse threats to the Army. The intelligence provided by this group has been critical to ongoing operations. The CIOC generates hundreds of reports of suspicious activity each year and "since 2011, there have been 10 incidents that resolved to a 'YES' nexus to terrorism and a full field investigation by the FBI."[103] The CIOC consists of four parts: the Investigative Analysis Branch, which handles large scale intelligence analysis and connecting with CID, DoD, and Army leadership at all levels; the Strategic Analysis Branch, which identifies crime trends; the Threat Analysis Branch, which consists of liaisons to other intelligence organizations and groups (such as the National Joint Terrorism Task Force); and the Field Analysis Branch, which consists of analysts working alongside field teams throughout the command.[104]

The CIOC ties into the larger intelligence section of CID, which includes criminal intelligence, data analysis, and crime prevention. Though CID does not handle Army counterintelligence (handled by the Military Intelligence Corps, or MI), the command's intelligence teams nevertheless provide critical support for all CID operations. The command expanded its pool of crim-intel analysts over the last few years and their capability to spot trends has grown as well. Utilizing various software suites and databases, these analysts can sift through this information and extrapolate patterns and averages in types of crimes and likely perpetrators. This ability has been bolstered by recent integration with the data systems of other MCIOs, broadening the information available to analysts. The Commander Risk-Reduction Dashboard is

[103] "DAHSUM, FY 2013," 17-19; "2014 Spring Semi-Annual Report to Congress," 32-34.

[104] "Command Intelligence Operations Center," U.S. Army Criminal Investigation Command, http://www.cid.army.mil/cioc.html.

a new tool that provides commanders with information on their soldiers, including data that may indicate they are a risk to themselves or others. Field agents also periodically conduct crime prevention surveys, looking for situations which are likely to lead to criminal behavior and stopping it before it escalates. All of these operations culminate in an annual crime report, which CID releases to the Army and DoD each fiscal year. Spearheaded by MG [redacted] these reports summarize the data and trends recognized by CID analysts and are given to senior leaders to assist in lowering and preventing crime throughout the Army.[105]

The DFSC, formerly USACIL, supports all of CID's operations through its institutional and expeditionary forensic capabilities. Since the mid-2000s, USACIL's mission had continuously been expanding and a move to broaden its capabilities finally came to fruition in November 2013, when it was officially redesignated as the DFSC. Under the new structure, the DFSC has four components. The first section, DFSC staff, fulfills various roles that support the lab's ongoing procedures, including Operations, Legal, Human Resources, Safety, Investigative Support, Information Management, Logistics, Resource Management, and Engineering. The second section, USACIL, maintains its dominant forensics functions, with sections dedicated to trace evidence, drug chemistry, latent prints, firearms and tool-marks, digital evidence, document forensics, serology and DNA, the Combined DNA Index System (CODIS), and evidence processing. The third section, the Forensic Exploitation Directorate (FXD), oversees the expeditionary elements of DFSC, including the Global Forensic Exploitation Center (GFXC), the Forensic Exploitation Teams (FXTs), and the Expeditionary Forensics Labs. The final section, the Office of the Chief Scientist (OCS), "is responsible for providing program management of all

[105] MG [redacted] interview, September 26, 2014, 3-4; Mr [redacted] nterview, October 17, 2014, 9-10; COL [redacted] phone interview, December 15, 2014, 5; Ms [redacted] interview, October 8, 2014, 2-6; "Ask the Chief," *The Shield*, July 2014.

forensic science related research, development, test and evaluation activities for the DoD for which the Secretary of the Army is the Executive Agent."[106]

DFSC receives and processes thousands of samples each year, analyzing evidence in the varied forensic categories listed above. During the reporting period, the lab instituted a new "Back in thirty" initiative, hoping to bring down turnaround time on lab analysis to a maximum of thirty days after receiving samples. The creation of the Forensic Case Management Branch (FCM) within the DFSC was instrumental in supporting this effort, which is still underway. One of the primary goals of the FCM Branch is to increase communication between agents and lab staff, with the eventually hope of creating an electronic tracking tool for agents to view the progress on their cases.[107]

An emerging area of the influx of forensics material is digital in nature. Even physical crimes will almost always have some kind of digital component connected to computers, cell phones, or the internet. The six digital forensics examiners at USACIL were becoming overwhelmed by the flood of digital samples in addition to physical ones. By increasing the training and certification of individual agents, SAs in the field were able to do preliminary analysis on digital evidence themselves. MG [redacted] pushed for the creation of more Digital Forensic Examiners at the team level, removing much of the burden from the DFSC and decreasing some of the backlog there.[108]

---

[106] Quote and information from [redacted], "USACIL now the Defense Forensic Science Center," *The Shield*, December 2013; further information from [redacted] interview, October 17, 2014, 3; "Command Brief," slides and accompanying information, U.S. Army Criminal Investigation Command, June 5, 2014, slide 24.

[107] USACIL, "Forensic Case Management Branch," *The Shield*, November 2014.

[108] MG [redacted] interview, September 26, 2014, 11-12, 22; Mr [redacted] interview, October 17, 2014, 8-11; [redacted] interview, October 15, 2014, 1-3; [redacted] interview, April 14, 2015, 2-3.

Nevertheless, forensics examiners at the lab had their hands full, tackling the massive amount of physical evidence, such as DNA. One of the main sources of samples has been Afghanistan (and before withdrawal, Iraq as well), which would send their evidence to the FXD. The GFXC serves as the reach-back point for surplus forensic evidence from Operation Enduring Freedom. They also analyzed evidence for a number of other bodies, including the Biometric Identity Management Agency (BIMA), Joint Task Force Guantanamo, and the Armed Forces DNA Identification Laboratory (AFDIL). During the reporting period, the GFXC received over 800 exploitation requests containing more than 5,000 items, in turn completing over 700 cases. The GFXC, working with the Naval Explosive Ordnance Disposal Technical Division, stood up its first resident explosive triage section. The FXD worked with BIMA (now DFBA) on several projects, including expanding their Automated Biometric Identification System (ABIS) through examining of latent-to-latent samples.

Fig. 8, FXD Caseload[107]

FXD Cases by Branch in support of OED, FY13	
Latent Prints	67
DNA	338
Electronic Engineer	29
Explosive Chemistry	35
Total	469

The other half of the FXD is the FXTs, deployable teams sent to analyze evidence in-theater. Team 1 operated in Afghanistan in FY13 and Team 2 deployed on November 28, 2013. The FXTs coordinated with the Afghanistan Captured Materials Exploitation (ACME) lab to process extensive forensic data. During the reporting period, ACME and the FXTs completed almost 5,000 requests from the field, encompassing more than 250,000 samples—including everything from DNA and latent prints to weapons and explosives. From this evidence, more than 1,200 insurgents were identified through the use of both the ABIS and AFDIL databases. In

[109] "DAHSUM, FY 2013," 9.

addition to numerous insurgents who were captured or killed in combat, these results led to the successful prosecution of approximately 300 individuals with a combined sentence of almost 3,000 years.

This expeditionary capability was built up during active combat, but now with operations declining, the OCO funding which supported this endeavor is declining. The reorganization of USACIL into the DFSC has helped to make the structure permanent, but the overall capacity is still in question. With the cuts referenced in Chapter 3 looming, the number of FXTs will be reduced drastically, though the demand for deployable forensic examiners persists. The capability will also be difficult to re-cultivate, as the costs—of both time and money—to train and prepare these examiners to conduct high quality tests in a hostile environment were very high.[110]

Though active combat in the Middle East is drawing down, it is not yet over. CID units deployed to Kuwait, Iraq, and Afghanistan throughout the last fourteen years. In addition to the FXTs, CID agents saw action on the frontlines. The 5th MP Bn (CID) made a historic deployment to Iraq in March 2011, the first time it had deployed since the Vietnam War. It was also one of the last of many CID battalions to serve in the region. U.S. Forces withdrew from Iraq in December 2011, and CID's mission there came to a close. Nevertheless, the command's operations abroad have continued in Kuwait and Afghanistan.[111]

---

[110] "DAHSUM, FY 2013," 8-13; "2014 Spring Semi-Annual Report to Congress," 4-12; MG [redacted] interview, September 26, 2014, 17-18; [redacted] interview, October 17, 2014, 3, 11; [redacted] interview, October 15, 2014, 5-6, 9; "Command Brief," slides and accompanying information, U.S. Army Criminal Investigation Command, June 5, 2014, slide 24.

[111] 5th MP Bn (CID), "5th MP Bn begins historic deployment," *The Shield*, May 2011; [redacted] "USF-I advise, assist efforts intensified," *The Shield*, January 2011; SGT [redacted], "MPs secure routes in Baghdad for last convoys," *The Shield*, February 2012.

Fig. 9, GFXC, FXTs, & ACME Forensic Testing, FY13 & FY14[112]

GFXC Activities

	Exploitation Requests	Items in Requests	Cases Completed
FY13	497	2,707	423
FY14 to date	307	2,616	308

GFXC Fingerprint and DNA Matching

	Total Latent Fingerprint Cases	Total Latent Fingerprint Examinations	New Latent Fingerprint Profiles	Database Matches from Fingerprints	New Searchable DNA Profiles	Biometric Matches from DNA Profiles
FY13	1,125	39,382	324	25	2,518	293
FY14 to date	662	14,498	46	7	2,021	257

Note: the Latent Print and DNA matches were utilized in support of the Combined Joint Task Force Paladin Theater Explosive Exploitation Cell, assisting in the assembly of thirty prosecution support packages.

DNA Identification by FXTs and ACME Lab

	Requests	Samples	Insurgents Identified	ABIS Matches	AFDIL Matches
FY13	3,367	209,561	735	543 (of 735)	192 (of 735)
FY14 to date	1,566	52,621	563	446 (of 563)	117 (of 563)

[112] "DAHSUM, FY 2013," 9-11; "2014 Spring Semi-Annual Report to Congress," 5-8. FY14 forensic data covers up to February 2014.

During the reporting period, the 19th MP Bn (CID) returned home, as did the 167th MP Det (CID). The 19th MP Bn had assumed duty from the 22nd MP Bn (CID) in the summer of 2012 and spent nine months in-theater. They were relieved in the spring of 2013 by the 11th MP Bn (CID), who were then reinforced by the 48th MP Bn (CID) and the 375th MP Det (CID). The 11th MP Bn and the 375th MP Det were subsequently relieved by the 502nd MP Bn, who arrived in-theater in the start of 2014.[113]

As discussed in Chapter 2, CID units, although soldiers, usually perform nontraditional missions in combat zones. They perform felony investigations, sensitive site exploitation, and support combat troops in other unconventional ways. An emergent area was logistics security, ensuring that Army supply lines remained intact and tracing stolen equipment. The geographic location of Afghanistan made maintaining supply lines difficult, due to being landlocked and bordered by nations who were not necessarily friendly to the United States. CID helped find stolen U.S. Government property and arrange "raids" with combat troops on stores and markets selling stolen materiel. They investigated attacks on Army installations, such as a suicide bomber attack on Forward Operating Base Gamberi in April 2011. CID also pursued drug crimes, digital crimes, and corruption, aided through deploying agents from the MPFU.[114]

Another initiative helping CID handle nontraditional operations is the Law Enforcement Professionals (LEP) Program. This program takes civilian contract individuals with extensive law enforcement experience and embeds them with combat troops. These individuals draw upon

---

[113] 19th MP Bn (CID), "Transfer of Authority in Afghanistan," *The Shield*, November 2012; 19th MP Bn (CID), "19th MP Bn (CID) Departs Theater," *The Shield*, July 2013; 11th MP Bn (CID), "375th MP Detachment (CID) Cases Colors," *The Shield*, July 2013; SSG (b) (6), (b) (7)(C), "11th Military Police Bn (CID) Returns Following Afghanistan Deployment," *The Shield*, February 2014; CPT (b) (6), (b) (7)(C), "502nd MP Bn (CID) Prepared for Deployment," *The Shield*, February 2014; (b) (6), (b) (7)(C), "CID Year in Review," *The Shield*, December 2013.

[114] SA (b) (6), (b) (7)(C), "840 kilos of poppy seized," *The Shield*, April 2011; (b) (6), (b) (7)(C) "CID puts the Taliban on notice," *The Shield*, August 2011; 10th MP Bn (CID), "Suicide Bomber Hits FOB Gamberi," *The Shield*, December 2011; (b) (6), (b) (7)(C), "Bagram's Digital Detectives Dig In," *The Shield*, September 2011; (b) (6), (b) (7)(C), "Combatting Corruption in Afghanistan," *The Shield*, August 2011.

their backgrounds to advise and mentor U.S., coalition, and local national troops on specialized topics to allow them to better meet the demands of fighting insurgents and their criminal networks. The LEPs are drawn from various Federal, State, and Metropolitan law enforcement organizations and are deployed to many troop levels, from corps and divisions to battalions and company headquarters. Their expertise includes investigative techniques such as interviewing and interrogation, evidence collection, and tackling the criminalized networks that support insurgents. LEPs have helped investigate various types of crimes, including thefts of Army supplies, tracking down bomb-makers, narcotics and drug trafficking, and more. Still, there were hurdles to success. LEPs worked best when they were able to deploy with their embedding force, rather than attempting to integrate later. They were able to provide the most insight and better serve the combatant commanders when fully enmeshed with the troops, which was not always the case. Also, the selection of LEPs must be a very deliberate process, ensuring that the individual is as skilled as they would appear on paper. A few seemingly highly qualified candidates were not as effective in-theater, while some of the most effective were investigators from smaller organizations, such as state police. Nevertheless, the LEP Program has been a success, leading to the prevention of attacks, disruption of insurgent networks, and successful prosecutions of enemy combatants.[115]

As Operation Enduring Freedom began ramping down, CID's mission remained critical to the war effort. CID agents helped in establishing a rule of law environment, as opposed to a purely active warzone. SAs policed Army installations, such as Kandahar Airfield, and carried out various nontraditional missions. Many operations involve prisoners, including the

[115] COL [redacted] interview, September 18, 2014, 13-14; "DAHSUM, FY 2013," 15-17; "2014 Spring Semi-Annual Report to Congress," 23-32; "Command Brief," slides and accompanying information, U.S. Army Criminal Investigation Command, June 5, 2014, slide 24. The LEP Program is administered by CID and supports both the U.S. Army and the U.S. Marine Corps.

interviewing and processing of captives, gathering intelligence and evidence of their crimes, and helping process the suspect through the Afghan criminal system. Agents also participated in the CID insert program which embeds an agent with combat troops, aiding commanders and soldiers in understanding the evidence collection process and helping them form a case which could be successfully prosecuted in local courts. This leads to another area of CID responsibility: aiding and training Afghan forces on proper law enforcement techniques. CID contributes to courses on evidence gathering, investigative techniques, and interrogation methods, often in conjunction with international trainers. CID worked with the FBI on the Major Crimes Task Force – Afghanistan, a joint operation designed to demonstrate for Afghan trainees how to pursue and convict suspects for "high-level crimes such as kidnapping, corruption, and organized crime."[116]

Another crucial component of drawdown operations which CID provides is crime prevention. Much like at home, CID units abroad perform investigations with the goal of preventing illegal activity and misuse of Army resources. Agents have conducted various crime prevention surveys in-theater, culminating in the creation of the Retrograde Operations Support Team – Afghanistan, or ROST-A. This team of CID agents monitors the removal of Army supplies and materiel from the theater and the transfer of bases and any designated equipment to Afghan National Security Forces. Initially a preliminary crime prevention team under by the 19th MP Bn, combatant commanders rapidly recognized the team's utility and integrated ROST-A into 1st Theater Sustainment Command, the primary headquarters for all retrograde operations in Afghanistan. ROST-A analyzes Army logistics and standard operating procedures as materiel is withdrawn or transferred, not only saving the Army money but also preventing resources from

[116] SA [redacted], "Gray Side Operations," *The Shield*, April 2012; [redacted], "Agents Under Pressure: Kandahar CID Det confronts crime," *The Shield*, May 2012; SA [redacted], "Major Crimes Task Force – Afghanistan: Attacking corruption through investigative mentoring," *The Shield*, August 2012; CPT [redacted] Afghan investigators take lead," *The Shield*, April 2013.

falling into enemy hands. Since its inception ROST-A has provided a cost avoidance to the Army of tens of millions, including the recovery of millions of dollars' worth of abandoned equipment of all kinds. They have gone through storage in Army installations such as Bagram Airfield, recovering supplies and ensuring thorough retrograde procedures. The team has also prevented dangerous disposal of excess equipment, in one case halting the burying of old uniforms which in turn could be recovered by enemy forces and used to impersonate friendly troops or infiltrate Army installations in the future. ROST-A reviews contractor operations and has gathered a great deal of information on suspicious activity for the MPFU to investigate. The team is also growing a crim-intel capacity, sharing the data it has accumulated from its surveys. This has been aided by a level three interpreter brought in from CITF, helping to coordinate the intelligence.[117]

The CITF is another critical element of CID's operations in-theater, with elements both abroad and at home. Originally created as a temporary joint task force between different branches under the CID CG, CITF was realigned as a permanent, purely Army task force reporting to the 701st MP Group commander on October 1, 2012. The move required shifting the funding out of OCO to the CID base budget, which in turn meant the total strength of the task force was reduced. Nevertheless, CITF has continued its founding mission, to support the military commissions in Guantanamo Bay in building the prosecution of its prisoners. CITF agents work in the field to gather evidence, passing it along to analysts who then sort through the data, in turn giving this information to attorneys who work with the DoD Office of the Chief Prosecutor (OCP) to help build solid cases.

During the reporting period, the CITF Document Media Exploitation unit analyzed hundreds of gigabytes of digital files, including videos, audio recordings, and text documents.

---

[117] MG [redacted] interview, September 26, 2014, 13; SA [redacted] 19th MP Bn (CID) creates ROST-A," *The Shield*, July 2013.

Since the creation of the unit, these analysts have combed through almost ten terabytes of digital evidence and over 400,000 documents. This evidence has been tied to more than forty terrorist-related cases. To meet the continuing demands of this mission, CITF expanded its digital forensics capability, bringing on two certified Digital Forensic Examiners, a CID civilian investigator, and an active-duty CID agent. These individuals deployed in the fall of 2013, supporting various law enforcement missions and gathering over 70,000 documents for use in future prosecutions.

CITF has been instrumental in building the cases against a number of high profile terror suspects held in Guantanamo. On June 7, 2013, Abd al Hadi al-Iraqi was officially charged for multiple acts of terrorism from 2001 to 2004. Al-Iraqi is suspected of being the head of Al Qaeda's forces in Afghanistan and Pakistan. He was charged with further acts of terror and retaliation against coalition forces from 2003 to 2004 on February 10, 2014. Ahmed Mohammed Ahmed Haza al Darbi was charged on February 5, 2014, for acts of terrorism including the attack on the French oil tanker *Limburg*, which resulted in the death of a Bulgarian crewman and the wounding of several others. He was arraigned on February 20, 2014. Ongoing litigation for other detainees include Abd al Rahim al Nashiri, who is accused of planning the 2000 bombing of the *USS Cole*, and Khalid Sheikh Mohammed, the alleged mastermind of the September 11, 2001 terrorist attacks.

Apart from its original function, CITF has expanded in many ways. In Afghanistan, deployed CITF agents have assisted the Combined Joint Interagency Task Force 435, which manages detainee operations. During the reporting period, CITF agents conducted almost 300 interviews, prompting over ninety percent of the detainees to confess. CITF also worked with the Afghan courts to bring those and other detainees to trial with successful prosecutions. Of the

over 1,200 trials, more than 800 resulted in convictions for various acts of terror. A new function in 2014 was the tasking of CITF staff to assist the OCP in building cases against fifty-three other-country nationals currently being held in Afghan prisons with alleged ties to the insurgency. Deployed CITF agents and analysts collected evidence and provided them to the OCP for further prosecution.

CITF also supported Task Force 2010 and the Section 841 process of screening current and potential contractors for connections to terrorism, the insurgency, or other criminal activity. Deployed CITF attorneys, aided by analysts at home, vetted almost 1,000 vendors in Afghanistan as part of Task Force 2010, leading to the denial of contracts to nearly ninety individuals and companies. CITF analysts and attorneys also investigated over twenty individuals and companies under Section 841, who were linked to $23,000,000 worth of government funds. In 2014, in conjunction with new NDAA legislation, a CITF attorney supported Task Force 2010 by analyzing a new Section 831 process which would expand the purview of the Task Force (and by extension CITF) to investigate contractors across all of CENTCOM's area of responsibility and five other combatant commands, not just Afghanistan. CENTCOM alone handles almost $13 billion in contracts which would now fall under Task Force 2010 and CITF's responsibility.

As mentioned above, CITF has provided support for ROST-A, which is a part of an emerging mission for not only retrograde operations, but logistics security in general. An agent and an analyst from the task force managed the LOGSEC desk at CID Headquarters in Quantico for much of the reporting period, managing and distributing information to CID and other law enforcement personnel in-theater. CITF analysts and agents aided the investigations of over a hundred CID cases in-theater, of which several dozen involved theft or other logistical crimes, eventually leading to the recovery of over $2.5 million worth of materiel. Task force personnel

analyzed retrograde supply shipping, finding vulnerabilities and preventing theft from cargo containers headed out of theater, as well as providing intelligence to recover addition stolen equipment.

Furthermore, CITF utilized the Logistics Security Common Operational Picture tool (LOGSEC COP), a software program that tracks valuable property in the battlefield. In the case of such valuable materiel being stolen, LOGSEC COP is designed to find the equipment and help organize operations to retrieve it. The tool was designed in house by CITF over the course of two years, saving the government from potentially spending millions of dollars to purchase similar programs. With development completed in 2013, CITF launched the program and used its features throughout the rest of the reporting period, tracking Army property as it was removed from the Afghan theater. They also shared the technology with the U.S. Department of Homeland Security Customs and Border Protection.

CITF agents, attorneys, and analysts have all worked with Afghan government and security personnel to stabilize conditions in preparation from the withdrawal of American troops. Much of this work has been with the Major Crimes Task Force, including mentoring and joint operations. Afghan investigators have helped CITF agents on LOGSEC operations, including a recovery mission of stolen industrial grade power generators and vehicle parts worth $1.5 million. CITF's expertise on insurgent and criminal networks is a valuable teaching tool, instructing Afghan investigators on techniques to battle corruption and trafficking. Analysts and attorneys from the task force have also assisted the Office of the Special Inspector for Afghanistan Reconstruction (SIGAR), providing data on insurgents and criminal activity which will be helpful in the future.

CIFT agents also support another crucial group—Army Special Operations. Though operations in Afghanistan have shifted towards rule of law over active combat, there are still missions that require the skills of more combat-oriented units, such as the Army Rangers. Special Operations units assault enemy targets throughout the theater, and while their objective is to engage enemy targets, they do take some enemy combatants alive, as well as discover evidence linking them and others to criminal activities. Despite such rule of law elements, these specialized combat units are not trained or equipped to optimally utilize the materials and information they secure. As such, CID agents under CITF deploy with Ranger battalions and other Special Operations teams in order to perform sensitive sight exploitation—gathering physical evidence and information to be utilized in a trial setting. This initiative has allowed more cases to be successfully tried and more enemy combatants to be convicted, especially in Afghan courts.[118]

However, these operations are not without risk. Especially in combat situations such as those faced by CITF agents with Ranger battalions, danger is an ever looming threat. On October 6, 2013, Special Agent Joseph M. Peters was killed in Afghanistan, the first CID agent to be killed in active combat since the command was established in 1971. SA Peters was deployed with the 75th Ranger Regiment, which was preparing to investigate a compound in the Zharay District of Kandahar in search of an insurgent leader. As they approached the compound, several suicide bombs and IEDs were detonated. The first line of soldiers was injured, and when their comrades moved forward to aid them, more explosives went off across the compound. SA Peter was among that second group rushing to help the wounded and was caught in one of the explosions. Three other soldiers were killed in the attack and thirteen were injured. Peters, 24,

[118] MG [redacted] interview, September 26, 2014, 10-12; COL [redacted] interview, October 15, 2014, 4-5; "DAHSUM, FY 2013," 13-15; "2014 Spring Semi-Annual Report to Congress," 12-23; [redacted] "CITF realigned," *The Shield*, February 2013.

enlisted in 2007 and joined CID in 2010. He had served in two prior tours in Iraq before his deployment to Afghanistan and had volunteered for the assignment to the 75th Ranger Regiment. He was awarded, posthumously, the Combat Action Badge, Bronze Star Medal with "V" device, Purple Heart, and the Meritorious Service Medal. He was honored during National Police Week in 2014 and, due to the work of the CID Public Affairs Office, his name was added to National Law Enforcement Memorial in Washington D.C. later that year. The November 2013 issue of *The Shield* published by the PAO was dedicated to his service. He is survived by his wife and young son.[119]

Even in light of such tragedy, CID has continued to pursue its mission both at home and abroad. They have pursued all manner of crime, from murder and suicide to hacking and fraud. They have protected prominent officials, analyzed crime trends, and been successful at preventing crime. They have battled sexual assaults. They have helped local populations and their fellow soldiers in Iraq and Afghanistan. They are part of a larger Army and law enforcement network, and their relationships to this community will be the focus of the next chapter.

[119] MG [redacted] interview, September 26, 2014, 24-26; [redacted] "Agent Killed in Afghanistan," *The Shield*, November 2013; [redacted], "Honoring the Fallen," *The Shield*, June 2014.

Chapter 5: Outreach

"Whereas CID always wears the black hat, I wanted to change that to the white hat, in which we are integrating and synchronizing and team players." MG (b) (6), (b) (7)(C) made this statement in reference to CID's reputation as being an isolated organization, a source of annoyance and complications for the average soldier and commanders at all levels.[120] Despite the critical nature of CID's investigative mission, the command's relations with the Army rank and file can be strained. In the words of CCIU Director, (b) (6), (b) (7)(C), "in many cases, CID is kind of that unwelcome knock at the door. If you're a mission commander and the phone rings from CID in the middle of the night, CID is typically not calling with good news."[121] However, through MG (b) (6), (b) (7)(C) leadership and the hard work of agents and staff across the world, CID has demonstrated that it is value added to the Army and is an integral part of the law enforcement community. Over the last several years, CID has worked to align itself with the rest of the Army and the Military Police family under the Provost Marshal General. The command has worked with its counterpart MCIOs and other law enforcement agencies to better combat crime, in addition to cooperating with the militaries of other countries and international organizations. CID has also looked to the public as well as looking inward, reaching out to members of the CID family and those around them. Overall, CID has exceeded far beyond simple investigations and their standard operations, connecting with the Army, the law enforcement community, and communities worldwide.

---

[120] MG (b) (6), (b) (7)(C) interview, September 26, 2014, 4.

[121] Mr. (b) (6), (b) (7)(C) interview, April 14, 2015, 12.

CID's relationship with the rest of the Army has been in flux over the past decade. When MG (b) (6), (b) (7)(C) revived the position of Provost Marshal General, he inserted the CID CG into the Pentagon allowing better connectivity with the rest of the Army, specifically access to the SECARMY and the CSA. With the addition of the ACC to their responsibilities a few years later, the PMG increased its prominence within the Department of the Army. MG (b) (6), (b) (7)(C) pushed to integrate even more with Army senior leadership, aided by a personal connection to the CSA; before serving as the Army Chief of Staff, GEN Odierno had been the commander of Multi-National Force – Iraq (MNF-I) and MG (b) (6), (b) (7)(C) served as the commander of Task Force 134 underneath him. Building upon this relationship, MG (b) (6), (b) (7)(C) was able to remain in contact with the CSA and by extension other senior Army leaders. In addition to meetings held three times a week, MG (b) (6), (b) (7)(C) also began sending weekly reports to the CSA, keeping him apprised of developments within CID and the other PMG commands. GEN Odierno liked the format of a concise status update on major developments and in turn made it a standard procedure for all the officers reporting to him to submit a weekly report based on MG (b) (6), (b) (7)(C) model.

MG (b) (6), (b) (7)(C) also pushed for CID to show its value and take on more of a client-based way of thinking in terms of dealing with commanders in the field. Having CID agents be a separate part of an installation or deployed unit and interacting with soldiers exclusively when they are being investigated was not an effective relationship. Instead, agents must be integrated fully into units, with the lead CID agent as a firm part of the commander's battle rhythm. Viewing the commander as a customer to CID, someone to cooperate with and lend support to, has greatly improved the perception of CID by the rank and file. CID agents are soldiers first, and the sharing of crime data and other resources with commanders has done much to reinforce

that, to foster the relationship between CID and its 'customers.' Especially in support of wartime operations, CID has truly shown its value to commanders, tackling not only murder and sexual assault but all of the nontraditional and unorthodox missions which CID has undertaken in Iraq and Afghanistan.

Now coming out of the wars in the Middle East, CID is trying to maintain this relationship, to ensure that they are still the "white hat." In the words of CSM [redacted], "CID is just a tool for the combatant commander." While this new outlook has become fairly engrained over the last several years, CID also must retain its independence. Though the bond with troops, commanders, and senior leaders should be strong, CID does have a unique position within the Army hierarchy. The command is an independent law enforcement agency and as such, is not bound by the commanders they support. They must pursue the evidence in their cases as they are, without interference by any other body. So while the client-mindset is good, it must not shift into an employee or command structure relationship. CID's integrity is crucial to its function as a policing body, and the command has done well to display its value while remaining objective.[122]

Nevertheless, CID is not alone within the larger Army system. It must work with other Army sections in order to gather information for investigations and other operations, and in turn to share the benefits of those cases with the rest of the Army. One of the primary methods of interaction is through the CID Liaison Program, also known as the LNO Program. This program consists of a number of liaison officers (LNOs) who connect CID with other organizations within the Army and federal government, to arrange for the transfer of important information to CID from other organizations and to update those organizations on the progress of relevant investigations. The LNOs are CID special agents who take on this additional responsibility and

[122] Quote from CSM [redacted] interview, October 15, 2014, 1; MG [redacted] interview, September 26, 2014, 2-6; COL [redacted] interview, October 15, 2014, 7-8; COL [redacted] interview, December 15, 2014, 7; LTC [redacted] interview, October 3, 2014, 7; COL [redacted] interview, September 18, 2014, 10.

are located either with or near their assigned organization. LNOs are primarily utilized under the MPFU, which has liaison officers working with the U.S. Army Corps of Engineers (USACE), the U.S. Army Material Command/U.S. Army Contracting Command (AMC/ACC), the Defense Finance and Accounting Service (DFAS), the Financial Crimes Enforcement Network (FINCEN), and the U.S. Transportation Command/Surface Deployment & Distribution Command (TRANSCOM & SDDC).

During the reporting period, the CCIU also integrated LNOs with the FBI National Cyber Investigative Joint Task Force; ARCYBER, which is responsible for all Army networks; and the U.S. Cyber Command (USCYBERCOM), which is responsible for all networks in the DoD. The LNO to USCYBERCOM, located at Ft. Meade, MD, additionally coordinates with the National Security Agency which is also headquartered at Ft. Meade. The command group and the new forensic psychiatrist, COL [redacted] are working to create a new LNO position with the Behavioral Analysis Unit (BAU) of the FBI, to foster additional cooperation and training in fields of psychology and behavioral forensics. COL [redacted] is also attempting to firmly establish a link between the command and the Center for Forensic Behavioral Sciences at Walter Reed, with the hope of bringing in fellows studying there to assist him with his investigations. The fellows already train with the BAU, and training with CID could provide them with additional experience and expand CID's forensic behavioral capabilities. Furthermore, CID has reached out to the Army at its earliest levels at the United States Military Academy at West Point (USMA). CID maintains an office at West Point and periodically hosts forums and presentations to the cadets there.[123]

[123] 701st MP Group (CID), "CID Liaison Program," *The Shield*, February 2013; 701st MP Group (CID), "CID Liaison Program," *The Shield*, April 2014; Mr. [redacted] interview, April 14, 2015, 8; [redacted], "The Facilitators: CCIU Liaison Officers," *The Shield*, May 2014COL [redacted] interview, March 30, 2015, 3-4; SA [redacted] "West Point CID helps educate future Army leaders," *The Shield*, January 2011.

To further its law enforcement capabilities, MG [redacted] utilized his position as Provost Marshal General to bring the Military Police Regiment closer together. Rather than having CID, the MP Corps, and ACC all be separate, disconnected bodies, the PMG began integrating some of their functions to boost efficiency and productivity. While each of these bodies remains distinct, MG [redacted] pushed for there to be more cooperation and sharing of information. MG [redacted] worked with the MP Corps to ensure that they and CID supported each other to the fullest extent on their parallel missions. Such efforts include the aforementioned combat support MPs utilized by the PSB and DSTs, as well as coordination with USAMPS to help these two groups to work better together. MG [redacted] also brought DFBA under the OPMG umbrella, adding a fourth hat to the position. Since the PMG oversees the DFSC under CID, MG [redacted] felt pairing the biometrics and forensics missions under the same authority would have beneficial results.[124]

Another poignant representation of solidarity among the MP family is CID's presence at memorials, specifically the Military Police Remembrance Ceremony which occurs each year on September 25. On this solemn occasion, CID joins the MP Corps and ACC—as well as representatives from other federal and state law enforcement agencies—to remember MPs that have been killed in combat that year, as well as honor all who made the ultimate sacrifice throughout the Corps' history. The Provost Marshal speaks at each year's Ceremony, which takes place in Arlington National Cemetery, and lays a wreath on the Tomb on the Unknowns to honor all fallen soldiers.[125]

---

[124] MG [redacted] interview, September 26, 2014, 2-6; Mr. [redacted] interview, October 3 2014, 7; [redacted] "USAMPS RCSM visits CID HQ and the 701st," *The Shield*, April 2012.

[125] [redacted], "Military Police Corps remember the fallen," *The Shield*, November 2012; [redacted] "Remembering the Fallen," *The Shield*, October 2013.

Beyond the Army and the MP Corps, CID works with the entire law enforcement community. Primary among its partner law enforcement organizations are its fellow MCIOs, including NCIS, OSI, and Marine Corps CID. Each agency is unique in its structure and operations, in addition to its own sphere of responsibility. Despite these differences, the MCIOs interact a great deal, further amplified by their current collocation in the Russell-Knox Building (RKB) in Quantico, VA. All MCIOs moved into this joint complex in 2011 with the intention of increasing collaboration and cooperation between these organizations. Initial results from the move are promising, though far from complete. Several sections have found great utility in working with their counterparts in other MCIOs—namely the human resources, logistics, and accreditations sections, as well as the Engineering and Safety positions. The CID G-6 has had the most success, integrating the CID computer systems and information technology with those of the other organizations in the RKB. The IT staffs worked together from an early point to design the shared cyber infrastructure they would be using. This process, and the management of the shared data centers once they were built, has created a strong bond between these departments. They have also shared a large amount of training. To a lesser extent, the G-3 and the intelligence sections have increased cooperation with their counterparts. Though certainly not integrated, the amount of shared information and coordination rose as a result of the move, particularly during the reporting period. This has led to assistance such as the Air Force suggesting better tablet models when CID was purchasing them for the command, as discussed in Chapter 3. The assistance is reciprocal; for example, OSI restructured their fraud unit during the reporting period, using CID's MPFU as a template.[126]

[126] MG [redacted] interview, September 26, 2014, 20-21; COL [redacted] interview, October 8, 2014, 3; Ms. [redacted] interview, September 18, 2014, 10-15; Ms. [redacted] interview, October 8, 2014, 5; Mr [redacted] interview, April 14, 2015, 3.

The move was also very beneficial for the CRC. Though their new facility in RKB is significantly smaller than at Ft. Belvoir, being located alongside their counterparts makes for easier access to records from other MCIOs. More prominently, the CRC underwent some reorganization as part of the move. Its employees increased in pay scale, providing opportunities for advancement and creating stability among the clerks. The CRC also merged its two main branches, consolidating responsibility and training. Not only did this improve the overall atmosphere of the workplace, but it also provided more flexibility—any clerk could handle any assignment given to them.[127]

Still, the new location is not without its problems. One significant detractor is the cost of the complex, which is approximately $2 million per year for CID. The previous headquarters at Ft. Belvoir cost under $200,000 per year for CID. Much of CID's staff like the new location as it has some nice amenities and is further south (out of the immediate Capital area), allowing for better commuting. However, due the distance, the CID CG is not as able to come to Headquarters as frequently he or she previously could. Since the CG spends most of his or her time at the Pentagon, it is difficult for him or her to come to the Headquarters more than once a week. The connectivity among the senior staff of the MCIOs is unfortunately not as tight as some of the smaller administrative sections. Senior leaders such as the Chiefs of Staff already had bimonthly or trimonthly meetings to discuss joint efforts between the MCIOs. Despite the fact that these leaders are now in close proximity and could meet more often, there has not been an increase in the frequency of such meetings. Much of this is due to how busy the staffs are; even with the factor of distance eliminated, their schedules are full and they are not accustomed to working as closely with their counterparts. This problem is even affecting some smaller

[127] Ms. [redacted] interview, March 30, 2015, 5-8.

sections, such as the G-8, which has also coordinated less with the budgetary sections of the other agencies.

The RKB presents a particular challenge to many of CID's operational elements. As the 701st MP Group is collocated with the Headquarters, several operational units—notably the MPFU and CCIU—also moved to Quantico. For the fraud unit, the Washington field office was moved from the relatively close location of Ft. Belvoir and moved considerably south. For the CCIU, their former facilities at Ft. Belvoir were specifically designed to house their hardware, such as advanced cooling systems and temperature control for their servers and other equipment. While their new facilities in Quantico are sufficient, they are not as extensive; this led to a number of incidents which damaged CCIU hardware and delayed their operations. For both the MPFU and CCIU, space is also a factor. The combined size of the Command Group, Headquarters staff, and the 701st has consumed much of the available CID sections in the RKB. For these two units with large-scale missions and planned growth, there is not much room to expand. There are plans being considered to address this issue, such as moving one or both of the units to an off-site location, but it nevertheless remains challenging for these units to act in their operational capacity when housed in a headquarters. The heightened security and cubicle setup are also not conducive to ongoing operations.[128]

Steps are being taken to strengthen the bonds among the senior leadership and take full advantage of the shared work environment. The Defense Criminal Investigative Organizations Enterprise-Wide Working Group, or more commonly called the DEW Group, is the main vehicle for this initiative. The DEW Group includes the Directors, Deputy Directors, Commanders, and DCOs of all the DCIOs and holds meetings on policy and high level decisions every six to eight

[128] [redacted] interview, April 14, 2015, 5; Mr. [redacted] interview, April 14, 2015, 9-10; COL [redacted] phone interview, April 6, 2014, 4; Mr. [redacted] interview, October 17, 2014, 7; CCWO [redacted] interview, October 24, 2014, 6.

weeks, supplementing the normal executive branch meetings that would occur annually. Though the DEW Group was originally conceived in the 1990s, it was not until the move into the RKB that it became a feasible and useful tool. The DEW Group already has made some headway in logistics, particularly forensic technology. They authorized the creation of the Procurement Efficiency Group at the behest of the Command FSOs of CID and OSI. The goal of this subgroup is to try to standardize forensic equipment used across the MCIOs. Standardization would be useful for future cooperation and joint missions, in addition to being significantly cheaper if all the agencies bought their equipment together. There is also a push, backed by COL (b) (6), (b) (7)(C) the CID DCO, to create an Operations subgroup of the DEW Group which would create and manage joint operations.

There is still much work to be done, and it is not a perfect situation. However, if CID and the other MCIOs make working together a priority, they can fully utilize their collocation. There are still downsides to RKB, such as the financial cost, but the move to a joint headquarters has already boosted camaraderie among personnel and led to unprecedented cooperation in some areas. For CID in particular, the new building provides a much higher level of security than what they previously had at Ft. Belvoir. It is doubtful that the agencies will ever consolidate into a single organization—and that is not being recommended by CID—but increased joint work will hopefully help all parties, in spite of their differences in structure and mission.[129]

Other endeavors for cooperation include efforts by the CIOC and the DFSC. The CIOC has boosted cooperation with its counterparts within other MCIOs, increasing shared intelligence analysis. 2013 saw the formation of the Joint Counterterrorism Coordination Cell (JC3), made of

---

[129] (b) (6), (b) (7)(C) interview, October 17, 2014, 7-8; CCWO [redacted] interview, October 24, 2014, 6-7; Ms. [redacted] interview, October 17, 2014, 8-9; Mr [redacted] interview, October 15, 2014, 7; COL [redacted] interview, September 18, 2014, 14-15; COL [redacted] interview, October 15, 2014, 8-10; Ms. (b) (6), (b) (7)(C), September 18, 2014, 10-15; Mr. (b) (6), (b) (7)(C), April 6, 2015, 6; COL [redacted] phone interview, April 6, 2015, 5.

members from CID's CIOC, OSI, NCIS, Army Counterintelligence and the Defense Intelligence Agency (DIA). This group supports the National Joint Terrorism Task Force (NJTTF) and the FBI to identify potential threats, including insider threats. The DFSC, through its FCM Branch, is continuously trying to increase communication between the lab and the law enforcement community. The branch's staff consists of various technical experts and liaison officers to not only CID, but also OSI and NCIS. The FCM Branch grew out of a pilot project originally created by OSI in July 2014. NCIS came onboard in October, and CID is slated to fully integrate with the FCM Branch in 2015.[130]

There are two computer systems that were developed during the reporting period that better connect CID to the law enforcement community. The new programs are the result of both MG (b) (6), (b) (7)(C) push to unify the MP family and the drive for cooperation among MCIOs in Quantico. The first, the DoD Law Enforcement Defense Data Exchange (D-DEx), is based on an NCIS program which was expanded through a joint process by NCIS, CID, and DoD. The new D-DEx program allows the DoD and ten other federal law enforcement agencies (including the MCIOs) to rapidly share information pertaining to cases, operations, and intelligence. CID and OPMG have also developed the Army Law Enforcement Reporting and Tracking System, commonly known as ALERTS, for use by both CID and the MP Corps. This is a case management system, storing and sorting ROIs from both organizations and letting CID and the MPs share information quickly and smoothly. Since both groups serve the Army, the merging of the two previous systems into one ensures that information is not trapped or lost in either system and reduces redundant data. After several years in development, the system was slated to launch

[130] "2014 Spring Semi-Annual Report to Congress," 33-34; USACIL, "Forensic Case Management Branch," *The Shield*, November 2014.

in the fall of 2014, though that date was pushed back to perfect the system. ALERTS went live on January 1, 2015.[131]

CID works with countless law enforcement agencies, including and beyond MCIOs. Another goal of MG [redacted] was to integrate and embed more CID agents in other agencies, to boost cooperation and capabilities. During the reporting period, MG [redacted] added two more agents into the Joint Terrorism Task Force and placed an agent within the FBI's Behavioral Analysis Unit. The majority of MPFU cases are joint, involving Defense Criminal Investigative Service (DCIS) or another MCIO, and the level of cooperation between the unit and its counterparts has risen dramatically over the last several years. Given the global scope of the CCIU's mission, they also actively work with partners throughout the law enforcement community, through the Defense Cyber Operation Group, which brings together senior cyber investigators from several MCIOs and other organizations, as well as an interface cell under USCYBERCOM which includes members from the FBI, DCIS, NCIS, OSI, the Coast Guard Investigative Service, and several other agencies. The CCIU, through the Technical Support Working Group, has given other agencies and law enforcement groups access to its REAP program. CID and the MP Corps have also worked a great deal with the U.S. Marshals Service. The Marshals Service has assisted in various training programs for the PSB, and MG [redacted] placed several Military Police officers with the Marshals Service. The pair of assigned MPs worked with the Marshals to create the Army Fugitive Task Force, a joint operation to track down soldiers who escape custody. CID provides information from Army databases about the fugitives, MPs work with Marshals to analyze the information and locate the fugitives, and then the Marshals use their resources to capture the fugitive and return them to the Army. To aid this

[131] Ms. [redacted] interview, October 8, 2014, 1-3; [redacted] "'ALERTS' Goes Online Fall 2014," *The Shield*, August 2014.

mission, the Task Force developed an Army Most Wanted list, the first of its kind. Originally including seventy five fugitives of various high level crimes such as murder and rape, the Army Fugitive Task Force has successfully captured about half of the individuals on the list.[132]

CID participates in various law enforcement gatherings and functions each year. Along with the other organizations under OPMG, CID is a regular attendee of the International Association of Chiefs of Police Conference and Exposition (IACP). At this event, representatives of CID participate in panels and discussions about law enforcement techniques and the specific challenges they face as an MCIO. They provide information about who they are and what they do to other law enforcement organizations on all levels from across the country, and even from around the world. Attendees also learn about other agencies and organizations in the community and network with them, fostering cooperative relationships. In June 2014, several CID agents traveled to Seoul, South Korea to attend the International Symposium on CyberCrime Response. Law enforcement agencies from over forty countries attended the event, hosted by the Korean National Police, with guest speakers from the FBI, Interpol, and more.[133]

Apart from the Army and other law enforcement agencies, CID also deals with various elements of the U.S. Government, notably DoD and Congress. The relationship with these bodies has improved somewhat over the last several years, much as it has with the Department of the Army. Having shown how valuable they are, especially during wartime, CID has gained more respect and appreciation from government officials. The senior leadership of CID has worked hard to maintain positive relationships with such officials, including MG [redacted] and COL

---

[132] MG [redacted] interview, September 26, 2014, 18-20; Mr. [redacted] interview, April 14, 2015, 3-5; Mr. [redacted] interview, April 14, 2015, 8-10; SA [redacted], "U.S. Marshals Service speaks to PSB Agents," *The Shield*, April 2012.

[133] [redacted], "Army law enforcement joins forces for IACP 2012," *The Shield*, November 2012; Surveillance Photos (3 of 9), *The Shield*, August 2014.

[redacted] CID has been open with Congress and other government bodies, sharing information about its operations and the crime data they have accumulated. While it may seem that media-heavy issues such as sexual assaults might be pushed by Congress and others onto CID, it has actually been more the reverse. CID has presented growing problems within the Army from an early stage—such as the increase in sexual assaults—allowing them to leverage the significance of these issues to gain additional resources and limit cuts. They also share information about their operations and investigation techniques, such as leading Congressional staffers on a tour of USACIL.[134]

CID outreach also extends beyond just the United States. Along with USAMPS, CID works with many of its international counterparts, often in the form of joint training operations. Such organizations include the Canadian Forces National Investigative Service, the Hessen Polizei of Germany, the Military Police of Slovenia, the Polish Armed Forces, and the Republic of Korea Military Police Investigators. CID and USAMPS held a five-day training session in Slovenia with their Military Police force from February 24 to 28, 2014, sharing techniques and discussing various law enforcement methods. CID agents participated in an international joint training program, BIOSAFE 2014, that summer in Poland. The five-day event consisted of simulations and field practice of optimal evidence extraction—gaining the most information without compromising the scene. Hosted by the Epidemiological Response Centre of the Polish Armed Forces, the event was also supported by the Illinois National Guard, the 7th Civil Support Command, U.S. Army Europe, and the 5th MP Battalion (CID). Hungarian and Slovakian military representatives participated as well. Members of the 19th MP Battalion (CID) and Korean Field Office (CID) conducted joint training sessions in mid-2014 with their counterparts

[134] COL [redacted] interview, October 15, 2014, 6-8; Mr. [redacted], October 17, 2014, 10-11; *The Shield*, May 2012.

from Korea, sharing polygraph research, digital forensics techniques, and visiting the Korean Military Police School. Later that year, a CID crim-intel analyst working under the 5th MP Battalion, SA [redacted], visited the headquarters of Interpol's Secretariat General located in Lyon, France. Along with three other analysts, the agent had a meeting with Interpol's Counter-Terrorism Fusion Center's crim-intel analyst. [redacted] said that the visit was a success, stating, "'This site visit allowed us to benefit from their Criminal Information System—which is the world's largest unclassified Terror/Crim-Intel Database, and obtain a partnership for future training support through various Interpol training programs within the AFRICOM area of responsibility.'"[135]

International outreach was a parallel part of CID operations in the Middle East theaters. CID units carried out several humanitarian missions in Afghanistan in addition to their military ones. Two in particular, Operation P.E.N.C.I.L. and Cat in the Hat, are designed to help children. Operation P.E.N.C.I.L. began in 2009 as a program to collect and disburse school supplies and other necessities to Afghan communities. The 22nd and 19th MP Battalions helped to gather supplies during their deployments, providing large amounts of supplies for students. The 19th MP Battalion also helped communities in Parwan province by constructing a number of "fuel donuts," a safe heat source made by compressing paper, sawdust, and water. The ultimate goal is to help the local populace build their own compression machine and teach them how to produce more of this environmentally safe and renewable heat source. Personnel of Bagram Airfield started Cat in the Hat in 2011. This is an educational program which brings children from in and

[135] LTC [redacted], "22nd hosts Canadian counterparts," *The Shield*, February 2011; [redacted], "German police train MPs to stop active shooters," *The Shield*, June 2011; CSM [redacted], "CID and USAMPS Partner with Slovenian Military Police," *The Shield*, July 2014; SA [redacted] & SA [redacted] "Special Agents Support Multinational Training Exercise in Poland," *The Shield*, August 2014; 19 MP Bn (CID), "19th MP Bn (CID) Visits ROK Counterparts," *The Shield*, September 2014; Surveillance Photos (10 of 10), *The Shield*, May 2014.

around Kabul onto the Airfield three times a week for basic English and math classes. Members of the 19th MP Battalion volunteered to help with the classes, providing the children with critical learning opportunities and building their relationship with and perception of the American military. Senior CID leadership also reached out in Afghanistan. MG [redacted] visited the theater multiple times during his tenure as PMG, meeting with CID, MP, and local Afghan forces. With the conclusion of active combat in the Middle East, much of these efforts have come to a close. Yet even now, CID agents are being deployed, this time to Africa, on a humanitarian mission. In November 2014, a pair of CID agents deployed to Liberia to aid Operation United Assistance, which is fighting to stop the spread of Ebola.[136]

One of CID's priorities is helping communities at home. Agents volunteer to aid veterans groups and speak at local schools about their jobs. Charity runs are a common volunteer activity, such as the Ft. Leonard Wood Sexual Assault Awareness 5K Run/Walk, in which several members of the 24th MP Det (CID) participated. Members of 68th MP Det (CID) joined hundreds of service members and civilian first responders in the Maryland Army National Guard's March Against Hunger on March 16, 2013. Several of the CID agents participated in the Norwegian Challenge as part of the march—completing the 18.6 mile course in full uniform and carrying a twenty-five pound rucksack. Many of the Challenge participants filled their packs with food to be donated to local food banks, totaling over 130 pounds of food. Another highly active group is "Team Justice," the volunteer program based out of 3rd MP Group in Georgia. Volunteers from this group have given back in many ways to the local community, including helping at homeless shelters and food banks. Members of Team Justice joined other military law enforcement units to

[136] "Operation P.E.N.C.I.L.," *The Shield*, July 2012; 19th MP Bn, "Bridging a cultural divide," *The Shield*, January 2013; "CID leadership visits MPs and agents in Afghanistan," *The Shield*, May 2012; [redacted], "MG [redacted] Looks to FY14 and Beyond," *The Shield*, January 2014; *The Shield*, August 2014; USMC 1LT [redacted] CID joins 101st Airborne Division for Ebola response mission in Liberia," *The Shield*, December 2014 (compiled).

participate in the Run for the Heroes event in 2013, a 260 mile relay across Georgia. The Run raised money for Houses for Heroes, a charity which supports veterans facing physical and financial hardship. The event raised over $160,000, with members of Team Justice and their comrades raising over $4,000. In 2013 and 2014, the 68th MP Det and CID PAO also joined other law enforcement groups during the 30th and 31st Annual National Night Out event. This celebration of law enforcement in the Capital area welcomes agencies and organizations of all types, allowing local residents to learn more about them. CID took full advantage of the opportunity to engage with the public, providing information about CID and its mission as well as demonstrations of its technical capabilities. In 2013, the 68th MP Det brought a crime scene trailer to share how they process a crime scene for fingerprints and other evidence. In 2014, they set up a display on bullet trajectory, blood splatter analysis, and crime scene reconstruction.[137]

In addition to all of CID's other outreach, from senior Army leadership and Congress to other MCIOs and international organizations, the command also looks out for its own. CID connects not only with its soldiers and civilian staff, but also their families and communities. The command publishes a monthly periodical, *The Shield*, which is produced by the Public Affairs Office. In addition to providing news and history important to the command, it is also a means to reach members of its community, providing public service announcements on a variety of topics. Some are more focused on aiding CID's mission, such as discussing operational security, handling classified materials, and avoiding copyright infringement, while many others focus on personal safety and emergency preparedness. CID has published articles to help soldiers and

[137] (b) (6), (b) (7)(C) "CID Agents lend a hand to veterans group," *The Shield*, June 2011; (b) (6), (b) (7)(C) "Special Agent talks to students about life behind the shield," *The Shield*, March 2012; Surveillance Photos (10 of 10), *The Shield*, June 2014; 68th MP Detachment (CID), "Marching for charity," *The Shield*, June 2013; 3rd MP Group (CID), "Chaplain's assistant leads 'Team Justice' volunteer efforts," *The Shield*, March 2013; 3rd Military Police Group (CID), "Team Justice takes on 260 Mile Run for the Heroes," *The Shield*, July 2012; (b) (6), (b) (7)(C) "Meade CID Spends the Night Out," *The Shield*, October 2013; (b) (6), (b) (7)(C), "National Night Out," *The Shield*, October 2014.

civilians deal with the stress of their jobs, as well as put out resources to help families cope with the stresses of Army life—especially when a family member is deployed. To keep up morale, CID hosts several community events during the year, such as an annual MP/CID Bass Tournament, which reached it twentieth year in 2013.[138]

CID also honors its soldiers and civilians for exemplary service. In recognition of fulfilling and exceeding their duties, members of CID are regularly awarded various medals and commendations. Members of CID are recognized by other organizations as well. SA [redacted] received special recognition as the 2014 DoD Task Force Officer of the Year. The award was granted by the Department of Justice. [redacted] was given the award for his outstanding service as part of the FBI Dallas Joint Terrorism Task Force, having done outstanding work with members of law enforcement beyond CID and providing a strong example of interagency cooperation. In addition to his overall efforts as part of the Joint Terrorism Task Force, [redacted] was especially recognized for a 2009 case pursued by [redacted] and his partner that revealed a number of translators working for the Army in Afghanistan were acting as double agents. These U.S.-born translators were secretly allied with the Taliban and were plotting against U.S. forces. [redacted] investigation led to the charging of three translators, two of whom have been convicted; the third was charged in August 2014 and is awaiting trial.[139]

---

[138] [redacted] Operations Security: Deception for protection," *The Shield*, July 2013; [redacted] "Copyright Guidance©," *The Shield*, November 2014; [redacted] "Emergency Preparedness," *The Shield*, September 2013; CSM [redacted] "From the CSM: Caring for Soldiers" *The Shield*, January 2014; [redacted] "How-to: Avoid Burnout," *The Shield*, January 2014; MG [redacted] "The CG Sends: Resiliency," *The Shield*, January 2014; MSG [redacted], "First Person Perspective: One agent's journey to get help," *The Shield*, January 2014; MG [redacted], "Commanding General Sends: The importance of family," *The Shield*, March 2014; [redacted], "Family Readiness: Tips from CID family members on how to live the 'CID life,'" *The Shield*, March 2014; [redacted], "FRG leader offers tips for success," *The Shield*, March 2014; News Brief, "2013 MP/CID Bass Tournament - 20th Year," *The Shield*, January 2013.

[redacted] "CID Agent Receives National Recognition in Fight Against Terror," USACIDC Press Release, September 11, 2014; [redacted], "CID Special Agent Receives National Recognition in Fight Against Terror," *The Shield*, September 2014. For further specific awards, see the "Surveillance Photos" and "CID Salutes" sections at the end of each copy of *The Shield*.

(b) (6), (b) (7)(C), Chief of the Family Advocacy Law Enforcement Training Division whose FETI technique was discussed in the previous chapter, was recognized by the End Violence Against Woman (EVAW) International Board of Directors in 2012. EVAW International is a global organization dedicated to educating law enforcement, the justice system, and the public about how to effectively battle gender-based violence, both through bringing perpetrators to justice and supporting victims. They presented [redacted] with their 2012 Visionary Award, which "is given to an individual who has advanced the field through research or practice, which as increased public awareness of the problem of violence against women and improved the response of criminal justice and community systems." [redacted] was presented with the award for his groundbreaking work in the field of sexual assault, including FETI and his extensive training of law enforcement professionals in a variety of organizations.[140]

Groups within CID are also recognized, such as the Forensic Exploitation Directorate under the DFSC. The FXD was presented with the August Vollmer Excellence in Forensic Science Award in late 2014 by the International Association of Chiefs of Police. The award is given "'to honor the proactive, innovative use of forensic technologies by law enforcement'" and elevating the use of forensic technology in the criminal justice system. The CCIU research and development team, led by SA (b) (6), (b) (7)(C), had previously been given this award in 2009 for the creation of their REAP program. The FXD received the award in recognition of their outstanding service in Afghanistan during combat operations, working in a battlefield environment and using forensics to help both law enforcement and the warfighter. In addition to their overall service, the FXD was also specifically recognized for their forensic support of the investigation of an attack on Camp Bastion and Camp Leatherneck on September 14, 2012. The

[140] (b) (6), (b) (7)(C), "Army Expert Receives National Recognition For Combatting Sexual Assault," USACIDC Press Release, January 17, 2012; (b) (6), (b) (7)(C), "Innovator in combating sexual assault receives national recognition," *The Shield*, February 2012.

perpetrator of the attack, which killed two U.S. Marines, was later apprehended due the efforts of the FXD and sentenced to death in an Afghan court—the first ever such conviction of an Afghan national insurgent by the country's criminal justice system.[141]

Another award of particular note was bestowed on a former CID agent, SFC Robert Keiser, on March 25, 2014. Keiser, known as "Cowboy Bob," was posthumously awarded the Distinguished Service Cross, the second highest Army award for valor. He passed away in 2009, and the award was accepted by his wife. The award was granted in recognition of his heroic actions in the Korean War, during a clash with enemy forces in the Kunu-ri-Sunchon Pass. Keiser was serving as an MP with the 2nd MP Company under the 2nd Infantry Division when they entered the pass, only to find the road blocked by a number of wrecked vehicles from a previous engagement and coming under heavy fire from enemy forces. While most of the soldiers were pinned down in their positions, Keiser ran to the front of the convoy and used the working vehicles to push the damaged ones into the ravine next to the road and open the path forward. For two hours, a wounded Keiser ran back and forth along the road under enemy fire, clearing the road himself and saving numerous lives. Keiser was heralded as a hero by his comrades and commanders, and was nominated for a Medal of Honor. However, due to a time limit on applications for such awards, Keiser's nomination was denied. Keiser, who had also served as an MP in World War II, went on to become a CID agent after Korea. He was finally granted an award for his actions due to the effort of one of his CID colleagues, who had pushed for his recognition for over a decade. This quest also led to the drafting of legislation to eliminate the two year limit on award nominations which had halted Keiser's original application.[142]

---

[141] (b) (6), (b) (7)(C), "Forensic Exploitation Directorate Recognized for Work in Afghanistan," *The Shield*, December 2014; (b) (6), (b) (7)(C), comp, "Computer Crime Investigative Unit (CCIU)," U.S. Army Criminal Investigation Command, updated 2015; Mr [redacted] interview, April 14, 2015, 8.

CID has a great impact on the lives of soldiers and their families, as well as on the law enforcement community as a whole. They work with the Army, the government, other law enforcement agencies, and even international groups to pursue their mission. They also give back to the community, participating in charity and local events, as well as supporting their own community through safety announcements, gatherings, and awards. CID works hard to maintain these relationships, allowing them to not only fight the battles of today, but also to prepare for those to come—the subject of the final chapter.

[142] (b) (6) (b) (7)(C) "Cowboy Bob: Former MP, CID Agent Awarded For Heroics," *The Shield*, May 2014.

Chapter 6: Forging the Future

"Every day you just cannot be looking at the twenty-five meter target. Anybody can shoot a twenty-five meter target."[143] MG [redacted] as evidenced by this quote, is an advocate of maintaining focus not only on the short term but also keeping a long term perspective. CID entered its forty-fourth year of operation as a major command in 2014 and by all indications will continue to pursue its mission well into the future. During the reporting period, CID has accomplished much—reorganizing its structure, handling new legislation, withdrawing from the Middle East, and more—but much still needs to be done. New policies are made every year, new technologies and techniques are introduced continuously, and the task of policing the Army never truly ends. As such, CID looks to 2015 and beyond to plan and manage its organizational structure, policy changes, resources and manpower, operations, and outreach.

CID is a unique organization, with the bulk of its personnel consisting of active duty military but also large sections of civilians. Despite its relatively small size, it has a global area of responsibility, requiring all personnel to work hard to achieve their goals. Though CID is a well-run and highly efficient organization, it still faces significant challenges. Agents and staff need to know their history and understand where CID comes from, to remind themselves of their duty. They also must be open-minded to new solutions and be wary of groupthink. Thankfully the command often has people come in from outside CID, especially in leadership positions, which helps to diversify perspectives and bring in new ideas. CID agents must retain their high

[143] MG [redacted] interview, September 18, 2014, 14.

standards of work and professionalism, and always look for ways to be better, ensuring that they remain among the top investigators in the country.[144]

Policies are always in flux. In the words of COL [redacted] "It's not like policy necessarily spikes and changes all of a sudden, but it is kind of a continuum that we are on. There's always going to be changes. You may think we've got everything just right, and there will be a tweak to something." CID must continue to adapt to this changing environment, handling shifts in legislation and focus. The command can also push for policy changes itself. Some specific issues that could be addressed include collateral misconduct, which can hamper investigations, and the revoking of benefits for families of convicted soldiers, which punishes innocent families for the crimes of their parent or spouse.[145] The shift from active combat to drawdown to peacetime must also continue. Policies aimed at supporting the war fight and sustainment, though necessary at that time, must be reevaluated and modified as necessary to prepare for the future.[146]

Another important area of policy to watch is certifications and training. CID has extensive training and certification programs in various fields. During the reporting period, they made significant strides in expanding these programs even further, such as with changes to the Forensics Master's Program and the FST course discussed in previous chapters. Nevertheless, there is still more that can be done. Agents need to have more psychological and forensic behavioral training to profile and track criminals. The addition of NCO polygraph examiners was a goal of 3rd MP Group that was not reached during the reporting period, but that could possibly be pursued in the future. Agents also need more leadership training and inter-agency experience

---

[144] COL [redacted] interview, October 8, 2014, 9; CSM [redacted], October 15, 2014, 8-9; COL [redacted] phone interview, December 15, 2014, 5-6; Mr [redacted] interview, October 17, 2014, 6-7; COL [redacted] interview, September 18, 2014, 3-4, 10-12; MG [redacted] interview, September 26, 2014, 22, 28.

[145] COL [redacted] interview, September 18, 2014, 4-7.

[146] COL [redacted] phone interview, April 6, 2015, 5-8.

to promote better cooperation within the law enforcement community. The push to have typical agents be better versed in physical and digital forensics has done well but needs to continue. Especially with digital forensics, agents must be able to analyze evidence effectively to increase efficiency, reduce reliance on the DFSC, and better handle cases. The addition of CCIU military agents is intended to help address this shortcoming and disseminate more digital expertise throughout the command, but whether this will be enough remains to be seen. Certifications for physical forensics are another area that requires more progress. Though programs such as the FST course are helpful, CID needs to be at the forefront of certifications, ensuring that all personnel are fully qualified to handle and process any necessary evidence. Otherwise, evidence—and by extension investigations—can be delayed or undermined. The process of developing new certifications must be deliberate and thought out, and the CID FSO is working with his counterparts to create better qualifications. The implementation of these certifications must also be a careful process, to ensure that agents do not find themselves needing specific qualifications in the field but have not had the opportunity to gain them.[147]

As detailed in earlier chapters, CID has access to varied resources to aid in their investigations, but is also about to suffer significant cuts to its budget and manpower authorizations. In terms of technology, the command has switched to electronic fingerprint scanners and hopes to implement full facial recognition and rapid DNA testing to booking stations in the next few years. Rapid DNA is an especially promising procedure, though it still requires more research and refinement before it can be fully relied upon. On the other side of forensics, CID and other MCIOs are working to meet the rise in demand for evidence storage.

---

[147] CSM [redacted] interview, October 15, 2014, 5, 9; COL [redacted] interview, March 30, 2015, 7; MG [redacted] interview, September 26, 2014, 20; COL [redacted] interview, December 15, 2014, 7-8; COL [redacted] interview, October 15, 2014, 10; Mr. [redacted] interview, April 14, 2015, 2-3; Mr. [redacted], October 15, 2014, 3-4, 8-9.

While the MCIOs have accommodated the initial wave of evidence brought on by new storage requirements accompanying recent legislation, these are mostly stopgap measures and more permanent solutions need to be found. CID and its counterparts are also working to improve the acquisition of new forensic equipment, ensuring that large purchases are necessary, practical, and fiscally responsible while staying current and meeting the demands of their operations. With forensic equipment and equipment as a whole, CID must continue to emphasize organization and standardization in its logistics, and maintain a dominant atmosphere of guardianship and accountability.[148]

Such caution and care is all the more important as CID draws down along with the rest of the Army. Funding for new projects and positions is difficult to come by and the available pool of money will likely only shrink over the coming years. As such, CID must maintain the efficient budget management it has carried out during the reporting period and continue to look for new ways to recoup funds and cover shortfalls. With regards to manpower, a similar approach must be taken, carefully analyzing what positions will be eliminated and how their responsibilities can be shifted to other positions. Reclaiming CID's lost growth will be a great challenge—though with cooperation from senior Army and government leadership, growth should continue, if at a considerably slower rate.[149]

Perhaps even more than policy and resource management, CID operations is a never-ending battle. Moving forward, CID will need to tackle several emerging problems. One of the most significant is sexual assault. While CID has made significant strides in investigating these cases, and new tools and techniques are regularly developed, there is still more that needs to be done. The problem of sexual assault is still on the rise and needs to be brought down. One

[148] [redacted] interview, October 15, 2014, 4-7; Ms. [redacted] interview, September 24, 2014, 3.

[149] Ms. [redacted], October 17, 2014, 10-13; Mr. [redacted] interview, October 3, 2014, 3-5.

possible aid could be the addition of more preventative sexual assault training for troops and CID agents alike. However, given the current constraints on manpower and resources, such training is difficult to make happen. Drug crime is another area that is on the rise. CID has taken steps to combat this trend, such as the increase in Drug Suppression Teams, but the problem will require more focus and resources for CID to assist the Army in overcoming it. CID also needs to refocus on economic crime, particularly on smaller scales. Due to the rigors of wartime, CID had to carefully prioritize its operations, and major cases such as violent crime, sexual assault, and large scale fraud were the main areas of focus after combat support missions. Now coming out of the war, the command can turn its view back towards thefts, fraud, and other economic crimes that were previously a lower priority. Furthermore, CID must continue to adapt to any new challenges that present themselves. The command has evolved; they no longer exclusively handle basic Title 10 investigations. Their methodologies, technologies, and mission now encompass much more than just that. In the Middle East, CID agents and analysts undertook rule of law operations and many other nontraditional missions, expanding the scope of what they can do. Emerging trends, such as the rise of megacities, will force CID—as well as the Army and the law enforcement community—to further expand their techniques and practices, to create new solutions.[150]

Keeping strong ties with the Army and the law enforcement community will aid CID in meeting these future challenges. CID joint operations in recent years, such as the Army Fugitive Task Force, have shown great promise and hopefully will continue to be successful. There is great potential for cooperation between CID and its fellow MCIOs, utilizing their shared location and organizations such as the DEW Group to maximize joint endeavors. Fostering this

[150] LTC [redacted] interview, 6; Mr. [redacted], October 17, 2014, 11; COL [redacted] interview, October 15, 2014, 10-11; MG [redacted] interview, September 26, 2014, 12-14, 26-27.

cooperation must be a priority to produce positive results. The command must also maintain close ties with the Department of the Army, with the Chief of Staff and the Secretary. MG [redacted] has been replaced by MG [redacted] GEN Odierno will transfer to another position in 2015. Nevertheless, the connectivity between the Provost Marshal General and the Department of the Army must be maintained, to perpetuate "momentum" between CID, OPMG, and the Department of the Army. The future leaders of CID must keep the viewpoint of "big tents," being open and active with the Army community. [151]

In 2013 and 2014, CID has pursued its mission across the globe. Agents have conducted varied operations to assist forces in and out of active combat. They have investigated crimes which threatened members of the Army family. The command has built up new capabilities in protective services, fraud, computer crimes, forensics, and more. CID has grown, reorganized, and enacted new policies, as well as built stronger bonds with the Department of the Army, its fellow MCIOs, and the law enforcement community at large. Together, CID has combined these forces to build a solid foundation to combat the challenges to come. "One, two, and three: support the current fight, assist and protect—our soldiers, our families, and our civilians—and then forge the future." These were MG [redacted] priorities when he assumed the position of Provost Marshal General and Commanding General of CID. All of these have been achieved, and now under MG [redacted] will move forward and continue to do what must be done. [152]

[151] COL [redacted] interview, October 15, 2014, 8-10; quotes and information from MG [redacted] interview, September 26, 2014, 23-24.

[152] MG [redacted] interview, September 26, 2014, 27.

Glossary

ABIS — **Automated Biometric Identification System**
Database of biometric data managed by BIMA; upgraded from version 1.0 to 1.2

ACC — **Army Corrections Command**
Responsible for Army Corrections system, including management of disciplinary barracks

ACME Lab — **Afghanistan Captured Materials Exploitation Lab**
Forensic facility located in-theater, processing materials from crime scenes in Afghanistan in support of Army, CID, and rule of law operations

AFDIL — **Armed Forces DNA Identification Laboratory**
Forensic facility located at Dover Air Force Base, providing research and examination of DNA evidence for DoD, military, and other members of the law enforcement community; under the Armed Forces Medical Examiner

AFIP — **Armed Forces Institute of Pathology**
Former forensic facility providing pathology expertise and services, especially in the field of forensic pathology, such as autopsies; disestablished in 2011

AFME — **Armed Forces Medical Examiner**
Medical organization supporting DoD and the U.S. military in medical-legal matters and laboratory investigative support, located Dover Air Force Base; oversees AFDIL, the DoD DNA Registry, Division of Forensic Toxicology, and more

AFRICOM — **United States Africa Command**
DoD/Army Unified Combatant Command (four-star) encompassing the theater of all African countries with the exception of Egypt; headquartered at Kelley Barracks, Stuttgart, Germany

ALC — **Advanced Leaders' Course**
Seven week course at Ft. Leonard Wood (USAMPS) providing training for MPs and CID agents to tackle challenges of leadership roles; successful completion of the course is one of the requirements for a 31D to become a 311A Warrant Officer

ALERTS	**Army Law Enforcement Reporting and Tracking System** New case management software system utilized by CID and the MP Corps, launched January 1, 2015; replaced the Automated Criminal Investigation/Intelligence System (ACI2) and features of the Centralized Operations Police Suite (COPS)
AMC/ACC	**United States Army Materiel Command/United States Army Contracting Command** Commands located at Redstone Arsenal, AZ responsible for supplying the Army with all needed equipment and items, through acquisitions and contracts with exterior businesses
ARCYBER	**United States Army Cyber Command** DoD/Army three-star command located at Ft. Belvoir, VA and Ft. Meade, MD, responsible for maintaining and defending Army networks; service component of USCYBERCOM
ATF	**Bureau of Alcohol, Tobacco, Firearms and Explosives** Federal law enforcement agency with diverse mission including illegal trafficking of alcohol, tobacco, firearms, and explosives, as well as investigating arsons, bombings, and acts of terrorism
BIMA	**Biometric Identity Management Agency** Former Federal law enforcement agency under OPMG responsible for managing biometric data; established in 2012 and redesignated as DFBA in 2013
CAIT	**Cyber Assurance and Investigations Team** CCIU Task Force established in 2013 to protect the digital records and public image of significant DoD and DA figures
CCIU	**Computer Crime Investigative Unit** Specialized CID unit under the 701st MP Group (CID) responsible for investigating intrusions into Army networks, monitoring internal threats and insider misuse, protecting the digital personas of protected HRPs, and carrying out crime prevention surveys of Army cyber systems.
CCWO	**Command Chief Warrant Officer** Advisor to the CID CG; highest Warrant Officer in the command, in charge of agent affairs for both Warrant Officers and enlisted personnel

CENTCOM **United States Central Command**
DoD/Army Unified Combatant Command (four-star) encompassing the theater of Southwest Asia and parts of Central Asia and North Africa; based at MacDill Air Force Base, FL

CG **Commanding General (CID)**
Commander of CID, usually held by a Major General; one of four command positions held by the Provost Marshal General

CID **Criminal Investigative Division**
Former title of USACIDC, also used by the Marine Corps Criminal Investigative Division (USMC CID); see USACIDC

CIOC **Command Intelligence Operations Center**
Nexus of CID's criminal intelligence capabilities, including collection, analysis, and dispersal of crim-intel throughout CID, the Army, and DoD

CITF **Criminal Investigative Task Force**
Formerly a joint task force with the mission of supporting prosecution of Guantanamo Bay detainees; its mission has since expanded to include combat support operations and sensitive site exploitation; became a reporting unit to the 701st MP Group (CID) in 2012

CJIS **Criminal Justice Information Service**
FBI facility in Clarksburg, WV which collects/processes information for the law enforcement community including case records and fingerprint data

CODIS **Combined DNA Index System**
FBI software and database of DNA and forensic samples used for comparisons by the law enforcement community

CRC **United States Army Crime Records Center**
CID facility collocated with CID Headquarters and the 701st MP Group (CID) in Quantico, VA, responsible for collecting, maintaining, and releasing Army law enforcement records; also written USACRC

CSA **Chief of Staff of the Army**
Military advisor to the Secretary of the Army and highest uniformed officer within the Department of the Army; occupied by a four-star General

CSM	**Command Sergeant Major** Advisor to the CID Commanding General; highest enlisted position in the command, in charge of NCO affairs
D-Dex	**DoD Law Enforcement Defense Data Exchange** Information-sharing program between DoD, MCIOs, and other federal agencies
DA	**Department of the Army** Federal agency under DoD which manages the U.S. Army, led by the Secretary of the Army
DAHSUM	**Department of the Army Historical Summary** Annual summary produced for the U.S. Army Center of Military History
DCIS	**Defense Criminal Investigative Service** DoD law enforcement agency; investigative branch of the Office of the Inspector General which pursues cases including corruption, fraud, cyber crimes, and supplying fraudulent equipment to the Armed Forces
DCO	**Deputy Commanding Officer** Refers to the Deputy Commander of CID, the highest officer under the CID CG; responsible for day-to-day operations of the command
DEW Group	**Defense Criminal Investigative Organizations Enterprise-Wide Working Group** Executive working group with members from all MCIOs and other DoD agencies; created to foster communication and cooperation between MCIOs
DFAS	**Defense Finance and Accounting Service** Federal agency which serves as the budgetary and finance arm of DoD
DFBA	**Defense Forensics & Biometrics Agency** Field Operating Agency under OPMG responsible for managing biometric data for DoD; established in 2013 as the new designation of BIMA
DFE	**Digital Forensic Examiner** Certification that can be acquired by CID agents signifying that they are able to effectively collect and analyze digital evidence

DFSC	**Defense Forensic Science Center** Forensic laboratory facility at Ft. Gillem, GA which serves DoD and the Army with traditional, reach-back, and expeditionary forensics capabilities; new designation of USACIL as of November 2013
DIA	**Defense Intelligence Agency** Military agency under DoD responsible for foreign intelligence and espionage; located in Washington, D.C.
DISA	**Defense Information Systems Agency** A combat support agency which provides and assists the law enforcement community with information technology, information management, and command and control
DMO	**Directed Military Overstrength** Temporary manpower authorizations (used for up to one year) allocated by the Department of the Army to support emerging or unforeseen needs
DoD	**Department of Defense** Federal executive department responsible for national security and military
DST	**Drug Suppression Team** Specialized teams of CID agents and combat support MPs that target criminal networks involved with trafficking and distributing of illegal drugs
EVAW	**End Violence Against Women** International humanitarian organization dedicated to raising awareness among law enforcement and the public about gender-based violence
FBI	**Federal Bureau of Investigation** Primary federal law enforcement and domestic intelligence agency of the U.S. government
FCM	**Forensic Case Management Branch** Section of the DFSC responsible for increasing efficiency and decreasing turnaround time on cases handled by the lab
FETI	**Forensic Experiential Trauma Interview** Specialized technique developed by Russell Strand to interview victims of sexual assault; gains maximum information with minimal harm to the victim

FINCEN	**Financial Crimes Enforcement Network** Bureau under the Department of the Treasury that investigates money laundering and other financial crimes
FIU	**Field Investigative Unit** Specialized CID unit under the 701st MP Group (CID) responsible for investigating sensitive and classified Army subjects
FLETC	**Federal Law Enforcement Training Centers** Interagency training facilities based from Naval Air Station Glynco, GA which provides programs for a variety of law enforcement groups at multiple levels
FOIA	**Freedom of Information Act (And Privacy Act)** Federal law that allows for disclosure of unclassified unreleased information by the U.S. government; "FOIA" also refers to the requests submitted by a citizen under this law to obtain government information
FORSCOM	**United States Army Forces Command** The largest Army command, which provides and produces conventional forces to meet the evolving needs of combatant commanders; based at Ft. Bragg, NC
FSO	**Forensic Science Officer** Designated CID Warrant Officer with specific forensic training and certifications, assigned at various levels; can also refer to the Command FSO, the primary forensic officer for all of CID
FST	**Forensic Science Technician** Certification for NCOs who have completed the Forensic Science Technician Training Program, a multi-phased training course which provides the NCOs with basic expertise in forensic crime scene analysis and proficiency with several forensic tools
FXD	**Forensic Exploitation Directorate** Directorate of the DFSC overseeing the Global Forensic Exploitation Center and Forensic Exploitation Teams; manages reach-back and expeditionary forensics, as opposed to more traditional tests managed by USACIL

FXT	**Forensic Exploitation Team** Deployable team(s) of forensic experts which can provide support in-theater through Expeditionary Forensic labs; subordinate unit to the Forensic Exploitation Directorate
GF	**Generating Force** Army forces which support and train operational troops; see OF
GWOT	**Global War on Terrorism** Collective term for combat and intelligence operations from 2001 to 2013, including the various sections of Operation Enduring Freedom
HRP	**High Risk Personnel** Senior DoD and DA leaders whose protection is provided for by CID—the PSB providing physical protection and the CCIU providing digital protection; such individuals include the Secretary of Defense, the Secretary of the Army, and the Joint Chiefs of Staff.
IACP	**International Association of Chiefs of Police** Multinational organization that fosters cooperation between various law enforcement groups and meeting the challenges that law enforcement will face in the future; the acronym can also refer to the annual conference held by this organization that is regularly attended by CID
IG	**Inspector General** The CID Inspector General oversees the operations and management of the command, ensuring that CID is in full compliance will all federal and Army policies and regulations
Interpol	**International Criminal Police Organization** Intergovernmental law enforcement organization dedicated to assisting cooperation between various national law enforcement groups; includes 190 member countries and headquartered in Lyon, France
JC3	**Joint Counterterrorism Coordination Cell** Multiagency DoD law enforcement group designed to increase collaboration and information sharing between MCIOs and DIA; established April 2013
JRTC	**Joint Readiness Training Center** Training center based at Ft. Polk, LA; utilized by units about to deploy to develop and enhance skills to be used on the battlefield

LEP	**Law Enforcement Professional** Member of the LEP Program; civilians with extensive law enforcement backgrounds in Federal, State, or Metropolitan organizations contracted by CID and deployed overseas to assist combat troops with rule of law operations
LOGSEC	**Logistics Security** Maintenance and protection of supply lines during combat operations, including the prevention of theft of and retrieval of government property
LOGSEC COP	**Logistics Security Common Operational Picture tool** Software program developed by CITF to track valuable materials in combat zones and assist in recovery if such items are stolen
LNO	**Liaison Officer** CID agent assigned to another command or organization with the additional duty to facilitate communication and cooperation between CID and that organization
MCIO	**Military Criminal Investigative Organization** Wing within each branch of the Armed Forces dedicated to investigating felony crimes involving their respective branches; their original missions have expanded to include other investigative operations as well; examples include CID, OSI, and NCIS
MI	**Military Intelligence Corps** U.S. Army intelligence organization, responsible for monitoring and analyzing intelligence; includes U.S. Army Counterintelligence; separate from CID
MNF–I	**Multi-National Force – Iraq** Official title of coalition forces that took part in Operation Iraqi Freedom from 2003 to 2009
MP	**Military Police** Refers to either the Military Police Corps, the designation of a member of this Corps (e.g., a single combat support MP), or a unit composed of Military Police soldiers; this organization is another law enforcement section within the Army, responsible for standard policing of Army installations and commands and investigating non-felony crimes.

MPFU — **Major Procurement Fraud Unit**
Specialized CID unit under the 701st MP Group (CID) responsible for investigating high level financial crimes which exceed $100,000 or whose scope exceeds the basic post, camp, and station level; also handles many financial crime investigations in-theater

(M)TOE — **(Modified) Table of Organization and Equipment**
DoD documentation which outlines the capabilities of a unit, including basic staffing and equipping requirements; "Modified" denotes a deviation from the base document, which occurs when a unit's needs vary based on a specialized mission (as is the case for CID)

NCIS — **Naval Criminal Investigative Service**
Navy MCIO responsible for felony investigations and intelligence operations, counterpart to CID; has a civilian investigative workforce as opposed to CID and OSI which utilize active duty agents

NCO — **Non-commissioned Officer**
High-level enlisted ranks including sergeant and corporal, below commissioned officers

NDAA — **National Defense Authorization Act**
Federal legislation passed annually which determines the budget for the Department of Defense; also includes mandated policy changes

NJTTF — **National Joint Terrorism Task Force**
Multiagency task force created by the FBI which oversees the numerous Joint Terrorism Task Forces throughout the U.S.; originally housed at FBI HQ, now located at the National Counterterrorism Center in McLean, VA

OCO — **Overseas Contingency Operations**
Collective term for continued combat and intelligence operations in the Middle East and beyond, replacing the term "Global War on Terrorism/War on Terror"; includes Operation New Dawn

OCP — **Office of the Chief Prosecutor**
Organization under DoD which is part of military commissions, consisting of attorneys and other legal staff from all military branches; works with investigative units (such as CITF) and brings charges against the accused

OCS — **Office of the Chief Scientist**
Directorate under DFSC which oversees program management for the lab, as well as forensic research and development for the DoD

OEF — **Operation Enduring Freedom**
Official title used by the U.S. Government for GWOT/OCO operations; includes various sections including operations in the Philippines, the Horn of Africa, and other areas, though it is primarily used in reference to combat operations in Afghanistan

OF — **Operating Force**
Army forces which carry out active operations; see also GF

OIF — **Operation Iraqi Freedom**
Codename for U.S. combat operations in Iraq from 2003 to 2010; now OND

OMA — **Operation and Maintenance, Army**
Primary funding for an Army command, for maintenance of equipment and installations and other sustainment purchases; usually granted by fiscal year

OND — **Operation New Dawn**
Title of U.S. combat operations in Iraq from 2010 to 2011, replaced OIF

OPMG — **Office of the Provost Marshal General**
See PMG

OSI — **Air Force Office of Special Investigations**
Air Force MCIO responsible for felony investigations and intelligence operations, counterpart to CID; has an active duty and civilian investigative workforce similar to CID; also written AFOSI

PBUSE — **Property Book Unit Supply Enhanced system**
Property accountability software system formerly utilized for logistics throughout the Army, including by CID

PMG — **Provost Marshal General**
Army staff position responsible for overseeing all investigations and incarcerations involving members of the Army; the position was reinstated in 2003 after being abolished for almost thirty years; since 2003 it has expanded its oversight, currently acting as the commander for CID and ACC, and recently added DFBA (on the orders of SECARMY)

PPO	**Protection Providing Organization** Approved groups legally responsible for handling the personal protection of HRPs; CID is a designated PPO
PSB	**Protective Services Battalion** Specialized CID unit under the 701st MP Group (CID) responsible for the protection of HRPs within DoD and DA; provides physical security services, threat analysis, and travel security; also provides protective details for foreign counterparts to senior DoD and DA personnel when visiting the United States on official trips
REAP	**Rapid Extraction and Analysis Program** Digital tool developed by the CCIU to remotely analyze a compromised computer and provide data back to their investigators
RKB	**Russell-Knox Building** Joint complex housing the headquarters of CID, its counterpart MCIOs, and other DoD investigative agencies located at Marine Corps Base Quantico in Quantico, VA; CID relocated to RKB from Ft. Belvoir in 2011
ROI	**Report of Investigation** Report filed by CID agents for each investigation they open
ROST–A	**Retrograde Operations Support Team – Afghanistan** Specialized CID team formed in Afghanistan to support the troop drawdown and the conclusion of combat operations in theater; conducts crime prevention surveys and monitors logistic security to ensure U.S. property does not fall into the wrong hands
SA	**Special Agent** The primary investigative force of CID, including NCO, Warrant Officer, and civilian agents; can also signify Secretary of the Army, see SECARMY
SECARMY	**Secretary of the Army** Head of the Department of the Army; a civilian position which oversees the entirety of the U.S. Army supported by the Chief of Staff
SIGAR	**Special Inspector General for Afghanistan Reconstruction** Group established by Congress in 2012 which oversees funds provided by the U.S. Government to Afghanistan for the purposes of reconstruction; audits, investigates, and reports on the disbursal of these funds

SOCO	**Standards of Conduct Office** CID offices which oversees agent behavior and investigates misconduct, comparable to Internal Affairs in other law enforcement agencies
SOUTHCOM	**United States Southern Command** DoD/Army Unified Combatant Command (four-star) encompassing the theater of South and Central America and the Caribbean; based in Doral, FL
TAA	**Total Army Analysis** Army process which examines force structure and plans for growth, reduction, and/or reorganization of commands and units; establishes requirements and suggested levels but does not provide funding
TDA	**Table of Distribution and Analysis** DoD documentation which outlines the manpower and resource needs of a unit beyond the specifications of a TOE/MTOE, or when a TOE/MTOE does not apply; used to meet the demands of new or emerging missions, such as the specialized functions of CID
TRADOC	**United States Army Training and Doctrine Command** DoD/Army four-star command responsible for developing operational doctrine and training of all Army soldiers; headquartered at Ft. Eustis, VA
TRANSCOM & SDDC	**United States Transportation Command & Surface Deployment and Distribution Command** DoD/Army Unified Combatant Command (four-star) which supplies transportation, via land, sea, and air to DoD and military personnel, coupled with its service component which coordinates and delivers supplies and equipment for troops as TRANSCOM moves them across the globe
UCMJ	**Uniform Code of Military Justice** Basis for U.S. military law, originally established by Congress; serves as the basis for courts-martial and all other military legal proceedings; is updated to address emerging issues
USACE	**United States Army Corps of Engineers** DoD/Army three-star technical command which oversees the construction and maintenance of all Army and Air Force installations (and their respective Reserve components) as well as the designing and construction of various civil engineering projects such as canals, dams, and locks; also abbreviated CoE

USACIDC **United States Army Criminal Investigative Command**
Army MCIO responsible for felony investigations (but not intelligence operations), utilizing primarily an active duty investigative workforce along with specialized civilian agents; originally named the Army Criminal Investigative Division (CID), the D remains as a historical reminder; the organization is still commonly called CID

USACIL **United States Army Criminal Investigation Laboratory**
Former title of the DFSC and currently the title of one of the lab's directorates; provides analysis for DNA, latent prints, trace evidence, and other traditional forensic support

USAMPS **United States Army Military Police School**
Training academy for the Military Police Regiment located at Ft. Leonard Wood, MO; offers a wide curriculum of courses including the CID Special Agent Course which all CID SAs must complete

USAR **United States Army Reserves**
Along with the Army National Guard, forms the reserve force of U.S. Army troops; reserve components can be mobilized as the need arises to increase the force strength of the Army

USCYBERCOM **United States Cyber Command**
DoD/joint military sub-unified command which monitors and defends federal, DoD, and military networks and cyberspace, based at Ft. Meade, MD; the commander of UCYBERCOM is also the Chief of the NSA; subordinate unit to United States Strategic Command (STRATCOM)

USFK **United States Forces Korea**
DoD/Army sub-unified command (four-star) which oversees all forces and operations in Korea, based out of the Yongsan Garrison, Seoul, South Korea; subordinate unit to United States Pacific Command (PACOM)

USMA **United States Military Academy at West Point**
Four-year Army training academy which teaches officers-in-training (cadets) who will enter active duty upon graduation; located in West Point, NY, the Academy is often called "West Point"

Bibliography

Interviews:

COL (b) (6), (b) (7)(C), September 18, 2014

Mr. (b) (6), (b) (7)(C) April 14, 2015

LTC (b) (6), (b) (7)(C), October 3, 2014

COL (b) (6), (b) (7)(C), December 15, 2014

COL (b) (6), (b) (7)(C) April 6, 2015

Ms (b) (6), (b) (7)(C), October 8, 2014

Ms (b) (6), (b) (7)(C), March 30, 2015

CSM (b) (6), (b) (7)(C), October 15, 2014

Ms. (b) (6), (b) (7)(C) September 18, 2014

Mr. (b) (6), (b) (7)(C) April 6, 2015

COL (b) (6), (b) (7)(C), October 8, 2014

COL (b) (6), (b) (7)(C), March 30, 2015

Ms. (b) (6), (b) (7)(C), September 24, 2014

Ms (b) (6), (b) (7)(C) October 17, 2014

Mr. (b) (6), (b) (7)(C) October 3, 2014

MG (b) (6), (b) (7)(C), September 26, 2014

Mr (b) (6), (b) (7)(C), October 17, 2014

Mr. (b) (6), (b) (7)(C), April 14, 2015

COL (b) (6), (b) (7)(C), October 15, 2014

CCWO (b) (6), (b) (7)(C) October 24, 2014

CCWO (b) (6), (b) (7)(C) (ret.), September 30, 2014

Mr. (b) (6), (b) (7)(C) October 15, 2015

PAO Materials:

CID Command Magazine, *The Shield*, 2011-2014

CID Command Website, http://www.cid.army.mil/

(b) (6), (b) (7)(C). "Army Expert Receives National Recognition For Combatting Sexual Assault." USACIDC Press Release, January 17, 2012.

(b) (6), (b) (7)(C) CID Agent Receives National Recognition in Fight Against Terror." USACIDC Press Release, September 11, 2014.

(b) (6), (b) (7)(C). "The Army's Digital Detectives: CCIU, Special Agent Recognized for Excellence." USACIDC Press Release, August 7, 2009.

(b) (6), (b) (7)(C) "Hunting the Hackers: CCIU Detectives Deliver Digital Justice." USACIDC Press Release, January 7, 2013.

Other Command Sources:

(b) (6), (b) (7)(C) editor. "CCIU Overview," slides. U.S. Army Criminal Investigation Command Computer Crime Investigative Unit, updated 2015.

(b) (6), (b) (7)(C)., comp. "Computer Crime Investigative Unit (CCIU)." U.S. Army Criminal Investigation Command, updated 2015.

"Command Brief," slides and accompanying information. U.S. Army Criminal Investigation Command, June 5, 2014.

(b) (6), (b) (7)(C). "United States Army Criminal Investigation Command, Annual Historical Review, Fiscal Years 2009 and 2010." R & D Associates, August 27, 2010.

(b) (6), (b) (7)(C). "CID Current Force (FY12 Authorizations)," slide. USACIDC Manpower and Force Structure Division.

(b) (6), (b) (7)(C). "CID Current Force (FY13 Authorizations)," slide. USACIDC Manpower and Force Structure Division.

(b) (6), (b) (7)(C) "CID Current Force (FY14 Authorizations)," slide. USACIDC Manpower and Force Structure Division.

(b) (6), (b) (7)(C) "Current Manpower and Force Structure Actions." USACIDC Information Paper, April 24, 2013.

(b) (6), (b) (7)(C) "Current Manpower and Force Structure Actions." USACIDC Information Paper, January 17, 2014.

(b) (6), (b) (7)(C) "Current Manpower and Force Structure Actions." USACIDC Information Paper, July 31, 2014.

"U.S. Army Center of Military History Department of the Army Historical Summary, FY 2013." U.S. Army Criminal Investigation Command, August 14, 2014.

"U.S. Army Criminal Investigation Command 2014 Spring Semi-Annual Report to Congress." U.S. Army Criminal Investigation Command, 2014.

External DA/DoD Sources:

(b) (6), (b) (7)(C) Col., United States Army. "Fiscal Year 2013 (FY13) Operation and Maintenance, Army (OMA) Funding Letter." Department of the Army memorandum, May 13, 2013.

"GCCS – Joint." Defense Information Systems Agency. http://www.disa.mil/services/command-and-control/gccs-j.

(b) (6), (b) (7)(C) Col., United States Army. "Fiscal Year 2014 (FY14) Operation and Maintenance, Army (OMA) Funding Letter." Department of the Army memorandum, February 27, 2014.

Soldiers, United States Army Chief of Public Affairs, June 2010. (Issue on USACIDC)

(b) (6), (b) (7)(C) MAJ, U.S. Army. "Total Army Analysis." Army Capabilities Integration Center. http://www.arcic.army.mil/Articles/cdd-Total-Army-Analysis.aspx.

Department of Justice Sources:

"Alleged Hacker Indicted In New Jersey For Data Breach Conspiracy Targeting Government Agency Networks." Department of Justice Press Release, October 28, 2013.

"Nine Defendants Plead Guilty in $20 Million Stolen Identity Refund Fraud Ring." Department of Justice Press Release, April 1, 2015.

"Twenty Million Dollar Stolen Identity Refund Fraud Ring Indicted." Department of Justice Press Release, May 22, 2014.