

Our Unit Logo

SYMBOLISM: The eagle and sword motifs are inspired by the seal for our parent unit, the 701st Military Police Group (CID). The eagle represents our law enforcement mission, while the sword represents our capabilities in time of war. The sword is fashioned as a lightning bolt to suggest the dynamic nature of our operations and the speed with which data traverses computer networks. The white star with red background is adopted from Army CID's shoulder sleeve insignia and distinctive unit insignia. The global map depicts our worldwide area of responsibility, and the binary code spanning the oceans suggests how computers and the Internet have bridged the gaps between continents. The circuit board design suggests a critical component of modern computers, and by extension, our operations. The Military Police Corps insignia is reimagined as wiring on the circuit board, symbolically suggesting our historical lineage and CID's command structure. The black and gold colors surrounding our logo are traditional U.S. Army colors and are central to the current U.S. Army logo.



About CID

With offices positioned around the world, CID's primary responsibilities are to investigate felony crime occurring against the U.S. Army or its personnel and to investigate matters with an Army nexus. Should you experience any criminal activity not related to a computer intrusion, please contact your local CID office. Additional information is available on the Internet at:

www.cid.army.mil

For computer intrusion or related incidents, please contact CCIU using the contact information on the front of this pamphlet.



www.cid.army.mil/cciu.htm

COMPUTER CRIME INVESTIGATIVE UNIT
U.S. Army Criminal Investigation Command



The Army's Digital Detectives

Contact Information:

9805 Lowen Road, Building 193
Fort Belvoir, Virginia 22060-5598

Phone: 703.805.2315 (DSN 655)

Fax: 703.805.2351 (DSN 655)

E-mail: cid.cciu@us.army.mil



"DO WHAT HAS TO BE DONE"



"DO WHAT HAS TO BE DONE"

Our Core Values

INTEGRITY – As stewards of the public trust, our words and deeds reflect what is legally, ethically, and morally right in pursuit of “Global Justice.”

PROFESSIONALISM – We set the standard for others within the cyber crime community, exhibit a courteous and conscientious bearing, and demonstrate respect for each other and our customers.

LOYALTY – We bear true faith and allegiance to the United States Constitution, our leaders, the United States Army, the Criminal Investigation Command, the Computer Crime Investigative Unit, and the citizens of this nation.

PERSEVERANCE – We are steadfast in our resolve to accomplish our mission, despite any obstacles, discouragement, or danger.

INNOVATION – We are leaders in the cyber crime community at finding better, smarter, and more effective and creative ways to operate, adhering to this formula for success:

INNOVATION = (IMAGINATION + EMPOWERMENT) × DARING

Our Operational Philosophies

FLEXIBLE STANDARDIZATION – Grants personnel a certain degree of latitude in employing procedures predicated on overarching general best practices.

DYNAMIC PROFESSIONALISM – Progressive and continuous efforts to ensure that personnel are properly trained and proficient, deliver legally sufficient work products that add value to investigations, and exceed customer service expectations.

Our Mission

INVESTIGATIONS – The CCIU’s primary mission is to conduct criminal investigations of intrusions and related malicious activities involving U.S. Army computers and networks. Because investigations of this nature require a level of computer expertise not usually found in most CID Special Agents, CCIU personnel receive advanced computer training from the Defense Cyber Investigations Training Academy, Federal Law Enforcement Training Center, and other providers.

FORENSIC ASSISTANCE – Certain CCIU Special Agents receive advanced training in processing and analyzing digital evidence. On a case-by-case basis, these experts assist other CID Special Agents, the U.S. Army Criminal Investigation Laboratory, and partner law enforcement agencies.

VULNERABILITY ASSESSMENTS – To assist the U.S. Army in maintaining the integrity and security of its networks, the CCIU has developed a Computer Crime Vulnerability Assessment (CCVA) program. This program identifies vulnerabilities considered to be crime conducive conditions and mandates corrective actions by the installation’s senior commander. By taking a proactive approach, the CCIU helps prevent future network intrusions and compromises.

CENTER OF EXCELLENCE – As the U.S. Army’s Center of Excellence for computer crime investigations, the CCIU provides centralized program management services and oversees training, professional development, certifications, promulgation of best practices, and customer feedback processes.

Our History

The CCIU was provisionally established as the Computer Crime Investigative Team (CCIT) in January 1998, in recognition of the expanding role of computers in criminal activities and investigations. The CCIT was created out of the Field Investigative Unit (FIU) and was given primary responsibility for investigating intrusions into U.S. Army computer networks. Prior to establishment of the CCIT, only a single forensic examiner at the U.S. Army Criminal Investigation Laboratory was dedicated to investigating computer crime, and field investigative expertise consisted of a few CID Special Agents with varying levels of advanced training or knowledge.

In September 1998, the CCIT became the Computer Crime Resident Agency (CCRA) and moved to Fort Belvoir, Virginia. In November 1999, the CCRA was re-designated as the Computer Crime Investigative Unit and separated from the FIU to become a subordinate element of the 701st Military Police Group (CID). In January 2000, the CCIU was officially established as a criminal investigative organization within CID.

Since its creation, the CCIU has been a key element in the successful prosecution of numerous computer intrusion matters, in addition to serving as an invaluable tool for protecting U.S. Army computer networks from intrusions and other malicious activities. The CCIU’s personnel have an international reputation as innovators in the areas of computer crime investigations and computer forensics.



“DO WHAT HAS TO BE DONE”



“DO WHAT HAS TO BE DONE”



“DO WHAT HAS TO BE DONE”