BY ORDER OF THE SECRETARY OF THE AIR FORCE

DEPARTMENT OF THE AIR FORCE MISSION DIRECTIVE 33

16 JULY 2021

DEPARTMENT OF DEFENSE CYBER CRIME CENTER (DC3)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **http://www.e-Publishing.af.mil** for downloading or ordering

RELEASABILITY: There are no releasability restrictions on this publication

---

OPR: SAF/IGX

Certified by: SAF/IGX
(Mr. James Penn)

Pages: 4

On 12 November 2020, by order of the Secretary of the Air Force (SecAF), the Department of Defense (DoD) Cyber Crime Center (DC3) was activated as a Field Operating Agency (FOA), effective 15 January 2021. This Directive states the mission, defines the organization and command structure, establishes the responsibilities for the DC3, and summarizes delegations of authority from SecAF to Director, DC3, as set forth in Headquarters Air Force Mission Directive (HAFMD) 1-20, *The Inspector General*. This Directive also rescinds Air Force Office of Special Investigations (AFOSI) responsibility as the designated focal point to coordinate administrative matters regarding DoD Executive Agent responsibilities, functions, and authorities for DC3 as specified in Air Force Mission Directive 39, Paragraph 3.18. Refer recommended changes and questions to the Office of Primary Responsibility using Air Force Form 847, *Recommendation for Change of Publication*. Ensure that all records created as a result of processes prescribed in this publication adhere to Air Force Instruction 33-322, *Records Management and Information Governance Program*, and are disposed of in accordance with the Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System.

1. Mission. DC3 is a DoD law enforcement (LE) and counterintelligence (CI) support activity delivering superior digital and multimedia (D/MM) forensic services, cyber technical and specialized training, vulnerability and cyber threat information sharing, technical solutions development, and cyber threat analysis in support of the following DoD mission areas: LE and CI investigations and operations; Cybersecurity (CS); Counterterrorism; Defense Critical Infrastructure Program (DCIP); Document and Media Exploitation (DOMEX); safety inquiries, and the full range of military operations.

2. Organization and Command. DC3 is designated as a Federal Cybersecurity Center, pursuant to National Security Presidential Directive 54/Homeland Security Presidential Directive 23, Cybersecurity Policy, and serves as the DoD Center of Excellence for D/MM forensics pursuant to DoD Directive (DoDD) 5505.13E, *DoD Executive Agent (EA) forthe DoD Cyber Crime Center (DC3)*, and DoDD 5205.15E, *DoD Forensics Enterprise (DFE)*. The DoD Chief Information Officer, through the DoD Senior Information Security Officer, serves as the principal staff assistant to DC3 in accordance with DoDD 5505.13E, provides overall guidance and develops policy for DC3 activities, and approves the addition or deletion of programs, functions, and activities for DC3 in coordination with the SecAF.

2.1. DC3 is directly subordinate to SAF/IG. The SAF/IG is limited to administrative guidance and oversight while DC3 retains its independent authority to conduct its mission areas.

2.2. The Director, DC3:

2.2.1. Is appointed by SecAF per DoDD 5505.13E and by operation of policy per Air Force Instruction (AFI) 36-901, *Civilian Senior Executive Management*.

2.2.2. Is designated a civilian law enforcement agent and maintains credentials as a special agent accredited by Air Force Office of Special Investigations (AFOSI) in accordance with Department of the Air Force Policy Directive 71-1, *Criminal Investigations and Counterintelligence*.

3. Responsibilities. DC3:

3.1. Director.

3.1.1. Exercises authority over all DC3 operations and assigned military, civilian, and contractor personnel.

3.1.2. Plans, programs, budgets, and executes all FOA resources and activities within DC3.

3.1.3. Represents the SecAF on the Defense DOMEX Council and Executive Committee.

3.1.4. As delegated in HAFMD 1-20, has independent execution of Executive Agent responsibilites for D/MM Forensics for those forensics disciplines associated with computer and electronic device forensics, audio forensics, image analysis, and video analysis.

3.2. Executes all the functions and responsibilities in DoDD 5505.13E.

3.3. As a Federal Cybersecurity Center, provides technical and all-source intrusion and forensics analysis of digital devices and media, cyber threat reporting, and cyber threat information sharing in support of the Defense Industrial Base (DIB), LE/CI investigations and operations, the US Intelligence Community, and federal agencies conducting cyberspace operations and national cyber incident response.

3.4. Is a National Media Exploitation Center partner organization and provides D/MM forensics laboratory services, forensic training and certification, and research, development, test and evaluation (RDT&E) services for DOMEX and serves as a member of the DOMEX Committee pursuant to DoDD 3300.03, *DoD Document and Media Exploitation (DOMEX)* and Intelligence Community Directive 302, *Document and Media Exploitation.*

3.5. Hosts the DoD-Defense Industrial Base (DIB) Collaborative Information Sharing Environment (DCISE) and serves as the DoD focal point for coordinating threat information sharing and measures to enhance the protection of unclassified DoD information transiting or residing on DIB information systems and networks in accordance with DoD Instruction (DoDI) 5205.13, *Defense Industrial Base (DIB) Cybersecurity (CS) Activities*.

3.6. Establishes DIB CS threat information sharing policies, processes, and standards and serves as the single DoD focal point for receiving DIB CS voluntary and mandatory cyber incident reporting pursuant to DoDI 5205.13 and Defense Federal Acquisition Regulation Supplement 252.204-7012.

3.7. Manages the DoD Vulnerability Disclosure Program, engages with the crowdsourced vulnerability research community, establishes policies and processes to validate and mitigate DoD Information Network (DODIN) vulnerabilities, and serves as the single DoD focal point for DODIN vulnerability reporting in accordance with DoDD 5505.13E and DoDI 8531.01, *DoD Vulnerability Management.*

3.8. Serves as a DoD representative to the National Security Council Vulnerabilities Equities Process in accordance with DoDI 8531.01.

3.9. Provides technical RDT&E of tailored software and complex system solutions to support digital forensic examiners and cyber intrusion analysts with tools and techniques engineered to specific requirements for the forensics process and LE/CI cyber investigations and operations.

3.10. Develops and delivers specialized cyber and investigative training and certification to protect DoD information systems and to support digital forensics examiners, cyber analysts, and cyberspace operations forces pursuant to the *DoD Cyber Workforce Framework,* DoDD 8140.01, *Cyberspace Workforce Management*, and *Joint Cyber Training and Standards*.

3.11. Provides D/MM forensic services, CI-oriented cyber training, and RDT&E of CI techniques in cyberspace in support of AFOSI and DoD CI programs and investigations in accordance with AFI 71-101 Vol 4, *Counterintelligence*, and DoDI S-5240.23, *Counterintelligence (CI) Activities in Cyberspace*.

3.12. Supports the DCIP through D/MM forensics services and all-source cyber analytics pursuant to DoDI 5240.19, *Counterintelligence Support to the Defense Critical Infrastructure Program (DCIP)*.

3.13. Subject to the administrative oversight of the SAF/IG, the SecAF has re-delegated to Director DC3 in HAFMD 1-20 the authorities necessary to execute DC3's assigned missions.

4. Delegations of Authority/Assignment of Responsibility. The authorities delegated and responsibilities assigned to Director DC3, as set forth in this DAFMD, may generally be re-delegated and re-assigned unless re-delegation or re-assignment is expressly prohibited by an attached delegation of assignment or superseding law, regulation, or DoD issuance. While Director DC3 may re-delegate authorities and re-assign responsibilities to other DC3 personnel, he/she will ultimately be responsible to the SecAF for all matters listed in **paragraph 3** of this publication. Any re-delegation of authority or re-assignment of responsibility made shall not be effective unless it is in writing. Any person re-delegating authority or re-assigning responsibility in accordance with this DAFMD may further restrict or condition the authority or responsibility being re-delegated or re-assigned.

SAMI D. SAID
Lieutenant General, USAF
The Inspector General