

# Report Suspicious Activity

Defense Hotline  
1-800-424-9098

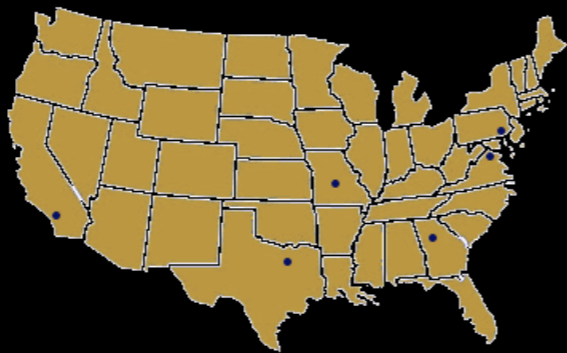


Contact the Defense Hotline to Report Instances of Criminal Activity Involving Technology Protection to Help Protect America's Warfighters

## DCIS HEADQUARTERS

Defense Criminal Investigative Service  
400 Army Navy Drive, Room 901E  
Arlington, VA 22202  
703-604-8600

## FIELD OFFICE LOCATIONS



Central Field Office 1222 Spruce Street Suite 8.308E St. Louis, MO 63103 (314) 539-2172	Southeast Field Office 1899 Powers Ferry Road Suite 300 Atlanta, GA 30339 (817) 303-6059
Mid-Atlantic Field Office 201 12th Street, South Suite 712 Arlington, VA 22202 (703) 604-8439	Southwest Field Office 2201 North Collins Suite 300 Arlington, TX 76011 (817) 543-4350
Northeast Field Office 10 Industrial Hwy Building Y, Suite 401 Lester, PA 19113 (610) 595-1923	Western Field Office 26722 Plaza Street Suite 130 Mission Viejo, CA 92691 (949) 643-4441

## OVERSEAS LOCATIONS

DCIS also has offices located in:  
Wiesbaden, Germany    Baghdad, Iraq  
Kuwait City, Kuwait    Bagram Air Base, Afghanistan

U.S. Department of Defense  
Office of Inspector General

# DCIS



## Operation Tech Defense

*Protecting America's Warfighters*

## MISSION

The mission of the Defense Criminal Investigative Service is to protect America's Warfighters by conducting investigations in support of crucial National Defense priorities.

## Protecting the Warfighters

Consistent with the mission of "Protecting America's Warfighters," DCIS is actively engaged in investigating the theft, diversion, and sale of sensitive military technologies. These technology protection investigations join terrorism, major procurement fraud, corruption, and protection of the Global Information Grid as a top investigative priority.

Technology Protection Program  
Office of Inspector General  
U.S. Department of Defense

# TECHNOLOGY PROTECTION

Protecting national security through investigation of the illegal theft, export, diversion or movement of strategic technologies and U.S. Munitions List items to proscribed nations, criminal enterprises and terrorist organizations that pose a threat to National Security.

This includes the illegal theft or transfer of technologies, weapons systems, components and programs, and all forms of high technology, information, and capabilities involving weapons of mass destruction.



# SAFEGUARDING TECHNOLOGY

The DCIS mission to protect the American warfighter extends to our industrial partners, who support our national defense efforts through innovative and superior products. Safeguarding the technological gains created by our private industry partners ensures both a thriving American economy and the safety of our Armed Forces.

Our efforts include collaborating with our law enforcement partners through various outreach programs such as Operation Tech Defense and Shield America.



# TECH PROTECT INDICATORS

DoD personnel, including contractors, military, and civilians, should report suspicious activity.

Warning signs could include...

- Customer pays in cash
- Products inconsistent with customer needs
- Shipping route is abnormal for the product and destination
- Purchaser is reluctant to provide end user information
- Declines installation or service contracts, warranties and installation on complex equipment
- Packaging is inconsistent with shipping mode, destination or product description
- Customer is unfamiliar with the product and has little or no business background
- A freight forwarding firm is listed as the final destination



Visit us on the web at:  
[www.dodig.mil/inv/dcis](http://www.dodig.mil/inv/dcis)

DCIS encourages DoD employees, contractor personnel, individuals serving in the Armed Forces, and the public to report criminal activity involving the protection of Department of Defense technology.

To Report Fraud, Waste, and Abuse Contact the Department of Defense Hotline at 1-800-424-9098



We need your assistance in providing any information relating to circumstances surrounding illegal export, diversion, theft or transfer of technologies, weapons systems, components and programs. This includes information or suspicious circumstances surrounding export transactions of high-technology items or services.