

## CYBER FIELD OFFICE

The DCIS Cyber Field Office is based in the Washington D.C. area and has dedicated Special Agents specifically trained in Cyber Crime spread across the continental United States. Our mission is twofold: investigating criminal cyber based offenses that affect DoD, specifically threats to the DoD Global Information Grid and the Defense Industrial Base, and providing digital media analysis and forensic support to DCIS for all investigations.



## DCIS HEADQUARTERS

★ **Defense Criminal Investigative Service**  
4800 Mark Center Drive • Alexandria, VA 22350-1500  
(703) 604-8600



### Central Field Office

1222 Spruce Street  
Suite 8.308E  
St. Louis, MO 63103  
(314) 539-2172

### Cyber Field Office

4800 Mark Center Drive  
Suite 14G25  
Alexandria, VA 22350  
(703) 699-7236

### Mid-Atlantic Field Office

4800 Mark Center Drive  
Suite 10D25  
Alexandria, VA 22350  
(703) 604-8439

### Northeast Field Office

10 Industrial Highway  
Building Y, Suite 401  
Lester, PA 19113  
(610) 595-1923/24

### Southeast Field Office

1899 Powers Ferry Road  
Suite 300  
Atlanta, GA 30339  
(770) 916-9920

### Southwest Field Office

2201 North Collins  
Suite 300  
Arlington, TX 76011  
(817) 303-6059

### Western Field Office

26722 Plaza Street  
Suite 130  
Mission Viejo, CA 92691  
(949) 282-2639

# DCIS

## CYBER FIELD OFFICE



**REPORT CYBER CRIME**  
cybercrime@dodig.mil

## PROTECTING THE WARFIGHTER

### MISSION

Conduct highly relevant, objective, professional investigations of matters critical to DoD property, programs, and operations that provide for our national security with emphasis on life, safety, and readiness.



**Fraud, Waste, & Abuse  
HOTLINE**  
Department of Defense  
[dodig.mil/hotline](http://dodig.mil/hotline) | 800.424.9098

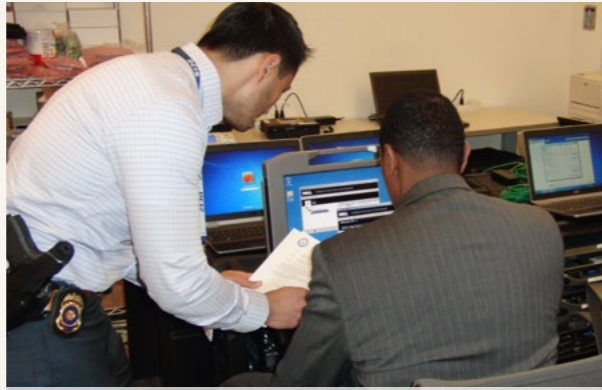
Office of Inspector General  
U.S. Department of Defense



## REPORT CYBER CRIMES

Your organization is on the front lines of a cyber war, and we need your help in protecting the U.S. Department of Defense by reporting suspicious computer and network activity. Providing DCIS with reports of illegal or abnormal activity affecting your organization's computers and networks can help us fight cyber crime.

Computer intrusions into the Defense Industrial Base put DoD and its warfighters at risk. These intrusions often include theft of data exposing sensitive defense data, such as advanced weapons system technology, to our nation's adversaries.



ELECTRONIC EVIDENCE ANALYSIS

The DCIS Cyber Field Office serves as a central point of contact to report cyber intrusions that impact the Department. DCIS special agents will respond appropriately to reported activity.

Contact DCIS to report illegal activity related to the Defense Industrial Base and the Department to include:

- Actual and attempted network intrusions
- Malware/spyware, botnets or viruses
- Social engineering attempts
- System compromises and data exfiltration
- Data destruction or alteration

[CYBERCRIME@DODIG.MIL](mailto:CYBERCRIME@DODIG.MIL)



ON-SITE INCIDENT RESPONSE



DIGITAL MEDIA EXAMINATION

## DID YOU KNOW...

- Hackers regularly target Defense Industrial Base companies rather than DoD and military systems directly, because they see DIB companies as "soft" targets.
- Reporting hostile activity to DCIS can assist in locating the attacker and help to prevent further incidents.
- Social engineering attempts (tricking employees into divulging information) identified by your organization should be reported to DCIS, even if they weren't successful.
- Portable computers or devices, including cell phones, which have been connected to networks outside your organization, can be used to attack your organization's network.
- Viruses, malware and spyware on systems, even if they don't result in the loss of information, should be reported.
- The breach of unclassified networks can be just as damaging to DoD as the loss of classified information. No breach is too small to report.
- Failure to report unauthorized access into your systems data may violate contractual agreements with the Department. Reporting these incidents can also help protect the interests and intellectual property of your organization.



CONTACT US  
Report Cyber Crime  
[CYBERCRIME@DODIG.MIL](mailto:CYBERCRIME@DODIG.MIL)