Cyber Task Forces

Building alliances to improve the nation's cybersecurity

The threat posed by terrorists, nation-states, and criminal groups conducting computer network operations against the United States has escalated to the point that it is widely considered a top national security threat. Protective measures being implemented by critical infrastructure operators, safekeeping of intellectual property by industry, and vigilance by citizens can only go so far. Unlike crime problems that may affect a single city or region, cyber threats are inherently national threats. Federal, state, and local authorities, along with international partners, must synchronize efforts to aggressively counter them.

National coordination of cyber threat investigations…

The 2008 Comprehensive National Cybersecurity Initiative (CNCI) created the foundation for a whole-of-government approach to protecting the nation from cybersecurity threats. As part of the CNCI, the National Cyber Investigative Joint Task Force (NCIJTF) was established under Presidential Directive as one of the country's national cybersecurity centers. Located in the Washington, D.C. area, the FBI-led NCIJTF serves as the national focal point for coordinating cyber threat investigations. In its role as a headquarters-level task force environment, the NCIJTF enhances collaboration and integrates operations among the represented U.S. Intelligence Community and federal law enforcement partners against:

- Cyber terrorists exploiting vulnerabilities in critical infrastructure control systems
- Nation-state theft of intellectual property and trade secrets
- Financially-motivated criminals stealing money, identities, or committing cyber extortion
- Hactivists illegally targeting businesses and government services
- Insiders conducting theft and sabotage

…comes to your community.

While national-level coordination is important to securing the nation, teamwork at the local level is also essential. After more than a decade of combating cyber crime through a nationwide network of interagency task forces, the FBI has evolved its Cyber Task Forces (CTFs) in all 56 field offices to focus exclusively on cybersecurity threats. In addition to key law enforcement and homeland security agencies at the state and local level, each CTF partners many of the federal agencies that participate in the NCIJTF at the headquarters level. This promotes effective collaboration and deconfliction of efforts at both the local and national level. The CTF role within the field office territory includes:

- Responding to cyber incidents and conducting victim-based investigations
- Understanding and addressing the threats, vulnerabilities, and collection opportunities that exist
- Maintaining relationships and information sharing with key companies and institutions

Each CTF also supports the national effort by:

- Providing surge capability for cyber incidents outside of the territory
- Participating in national virtual teams on a topic or threat
- Contributing subject matter experts for instruction, presentations, and research/development projects

CTF Mission

In support of the national effort to counter threats posed by terrorist, nation-state, and criminal cyber actors, each CTF synchronizes domestic cyber threat investigations in the local community through information sharing, incident response, and joint enforcement and intelligence actions.

Join us in partnering for a more secure future.

Successfully countering threats to the nation's cybersecurity requires a multi-disciplinary and multi-stakeholder team approach, and your local CTF values your contribution. By participating in the CTF, your agency's mission will be enhanced through:

Understanding the Threat

The threat landscape is constantly changing, and what your agency doesn't know can hurt those you are dedicated to protecting. By joining the CTF, your personnel will have access to real-time classified reporting.

Training Opportunities

Participants gain access to the FBI's cyber investigations curriculum, comprised of dozens of internally-developed and industry certification courses.

Access to Resources

For state and local partners, officer overtime, lease vehicles, fuel, smart phones, and computer equipment are available.

For more information, contact your nearby FBI field office or visit **www.fbi.gov**.