

STOP.THINK.CONNECT.™

Department of Homeland Security Component Overview

OVERVIEW

The growing number of attacks on America's cyber networks has become, in President Obama's words, "one of the most serious economic and national security threats our nation faces." The Department of Homeland Security (DHS) plays an important role in countering these threats. Since its founding in 2003, DHS has worked to build a skilled, effective team to keep the country's federal civilian networks secure and to protect critical cyber infrastructure on which all Americans depend for daily functions.

The Stop.Think.Connect.™ Campaign is one of the primary outreach efforts used by DHS to fulfill its cyber mission and promote awareness about online safety to the general public. The Campaign, initiated by President Obama in the 2009 Cyberspace Policy Review, seeks to guide the nation to a higher level of Internet safety by empowering the American public to be more vigilant about practicing safe online behavior.

DHS COMPONENTS

The Stop.Think.Connect. Campaign engages with many of the DHS operational components to raise awareness about cyber threats and to promote the use of safer online practices.

- **U.S. Customs and Border Protection (CBP):** CBP prevents terrorists and terrorist weapons from entering the United States and ensures the security of the nation's borders and ports of entry. CBP is also involved in the DHS cyber mission through its work to protect American businesses from intellectual property theft. As part of their efforts to stem this theft, CBP facilitates and ensures the safety of international trade, collects import duties, and enforces U.S. trade laws.
- **Federal Emergency Management Agency (FEMA):** FEMA's mission is to support the American people as well as first responders to ensure that the nation works together to build, sustain, and improve its capability to prepare for, protect against, respond to, recover from, and mitigate all hazards, including debilitating cyber attacks. FEMA maintains the Ready.gov website, which among other things, provides tips about cyber and all hazards preparedness. FEMA also facilitates National Level Exercises, some which have cyber components, to test emergency readiness.
- **Immigration and Customs Enforcement (ICE):** ICE, the largest investigative agency in the U.S. Department of Homeland Security (DHS), protects national security by enforcing the nation's immigration and customs laws. One of ICE's leading priorities is to combat criminal activity conducted on or facilitated by the Internet. The ICE Cyber Crimes Center (C3) delivers computer-based technical services to ICE components to support domestic and international investigations into cross-border crime. ICE also runs Operation Predator, an initiative to identify, investigate and arrest online child predators and sexual offenders.



STOP | THINK | CONNECT™

- **Transportation Security Administration (TSA):** TSA is responsible for security at the nation's airports and deploys a federal workforce to screen all commercial airline passengers and baggage. TSA employs a risk-based strategy to secure U.S. transportation systems, working closely with stakeholders in aviation, rail, transit, highway, and pipeline sectors, as well as the partners in the law enforcement and intelligence community. TSA also regularly contributes to the DHS cyber mission by assessing and updating cyber security protocols and programs to ensure the protection of both public and private data sources.
- **U.S. Coast Guard (USCG):** The USCG is one of the five armed forces of the United States and the only military organization within DHS. Since 1790, the USCG has safeguarded the nation's maritime interests and environment around the world. In addition to assisting U.S. Cyber Command, the USCG maintains the Coast Guard Cyber Command, which works to protect the nation's maritime critical infrastructure from online threats. The USCG is an adaptable, responsive military force of maritime professionals whose broad legal authorities, capable assets, geographic diversity and expansive partnerships provide a persistent presence along America's rivers, in the ports, littoral regions and on the high seas.
- **U.S. Secret Service (USSS):** The USSS mission is twofold. First, USSS safeguards the nation's financial infrastructure and payment systems to preserve the integrity of the economy. Second, the USSS protects national leaders, visiting heads of state and government, designated sites, and national special security events. As part of its first mission, USSS maintains Electronic Crimes Task Forces (ECTFs). The concept of the ECTF network is to bring together not only federal, state and local law enforcement, but also prosecutors, private industry, and academia. The common purpose is the prevention, detection, mitigation, and aggressive investigation of attacks on the nation's financial and critical infrastructures.

FOR MORE INFORMATION

By engaging with the DHS Stop.Think.Connect. Campaign, you will have the opportunity to join in cybersecurity awareness efforts with all seven DHS components. If you or your organization is interested in working with the Stop.Think.Connect. or any DHS components, please contact the Campaign at stopthinkconnect@dhs.gov.



**Homeland
Security**



STOP | THINK | CONNECT™