Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated December 19, 2018

DHS's Cybersecurity Mission—An Overview

Much of the U.S. government's cybersecurity apparatus focuses on the adversary—the person or organization that seeks to or has already carried out an attack against information technology (IT) systems. The U.S. Department of Homeland Security (DHS) is unique in the government's structure because its work to ensure national cybersecurity is largely agnostic to any individual threat actor, but informed by the risks that the actor presents. This In Focus describes DHS's cybersecurity missions and how the Department interacts with others to accomplish its missions.

DHS's Cybersecurity Missions

DHS has a variety of cybersecurity missions, which span the spectrum of prevention, protection, mitigation, response and recovery. In operating along this spectrum, DHS seeks to assess cyber risks and use its understanding of those risks to promote security and resilience of information communication technology (ICT) systems. When a cyber incident occurs, DHS has capabilities and authorities to provide direct assistance to the victim (both federal and non-federal) to help that victim recover from the incident.

Information Sharing

DHS seeks to improve the cybersecurity of the nation by sharing information among federal entities and with non-federal entities (e.g., state governments and the private sector). This can be classified information from an intelligence community source, sensitive information from an industry partner or unclassified information that is being promulgated through DHS's communications channels. However, information sharing by itself does not improve cybersecurity, but requires someone (e.g., a system administrator or an end user) to change a behavior in response to learning the shared information.

Federal Network Security

DHS monitors for threats against federal agencies and takes actions (either unilaterally or in collaboration with other agencies) to respond to threats. DHS can block malicious Internet traffic before it enters an agency, inform an agency when it has a vulnerability, direct agencies to mitigate threats, and provide technical assistance to agencies to respond to cyber risks. The Federal Information Security Modernization Act of 2014 (P.L. 113-283) codified the role that DHS plays in securing federal networks (along with the role that OMB, the NIST, and the individual agencies play).

Critical Infrastructure Protection

DHS identifies entities among the 16 critical infrastructure sectors (as set forth in Presidential Policy Directive 21) and works with them to mitigate risks, regardless of whether those risks are natural (like a hurricane) or man-made (like a cyber attack). DHS conducts risk assessments of entities, provides technical assistance to achieve security (before, during and after an incident), and shares information with entities to encourage changes in security postures. The department does this as part of the critical infrastructure protection mission granted to DHS as part of the Homeland Security Act of 2002 (as amended, P.L. 107-296) and as part of specific cybersecurity authorities granted in the National Cybersecurity Protection Act of 2014 (P.L. 113-282), the Cybersecurity Act of 2015 (P.L. 114-113, Division N), and the Cybersecurity and Infrastructure Security Agency Act of 2018 (P.L. 115-278).

Law Enforcement

DHS can investigate a variety of cybercrimes through the department's law enforcement agencies. These crimes include those enabled by the use of ICT, such as intellectual property theft or financial theft. Increasingly, criminal endeavors carry a cyber element, such as the smuggling of money across borders through the use of cryptocurrencies and stored-value cards.

Research and Development

Through its components and the Science and Technology Directorate, the department funds research and development into technologies with the objective of improving cybersecurity and transitioning those technologies to wide adoption.

Mission Execution by DHS Components

There are many entities within DHS that execute the department's cybersecurity mission. Below are a few DHS components with cybersecurity roles.

Cybersecurity and Infrastructure Security Agency

CISA is the primary component involved with cybersecurity. Congress created it from a previous component (P.L. 115-278). Through the National Cybersecurity and Communications Integration Center (NCCIC), DHS's cyber watch center, the department coordinates civilian cybersecurity activities and serves as the primary interface between the non-federal entities and the federal government. Within the NCCIC are the U.S. Computer Emergency Readiness Team (US-CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) which find and develop mitigating solutions against cyber threats. CISA also performs stakeholder outreach, develops policies and implementing guidance for federal agency cybersecurity, and deploys tools for cybersecurity. CISA is also the sector specific agency for many sectors, including IT, Communications, Dams, Nuclear Facilities, and Government Facilities (including election infrastructure).

U.S. Secret Service

USSS investigates crimes against the financial sector and threats online and in IT as part of its mission to protect the President and dignitaries.

Immigration and Customs Enforcement
ICE's Homeland Security Investigations (HSI) investigates crimes on the Internet such as intellectual property theft, currency smuggling and child exploitation, among others.

Transportation Security Agency
TSA, as the sector-specific agency for the transportation sector, has the responsibility to assess risks to the sector, share information on mitigating those risks and coordinate activities for risk mitigation.

U.S. Coast Guard
USCG, as the sector-specific agency for the maritime sector, assesses risks to the maritime industry, shares information, and works with the industry to mitigate those risks. Additionally, as a military branch, USCG has further cyber responsibilities to the Department of Defense.

Federal Emergency Management Agency
FEMA, as the agency responsible for emergency response, worked with the predecessor to CISA to develop the National Cyber Incident Response Plan (NCIRP) and ensure it aligns to the doctrine established in the National Response Framework (NRF).

Specific Programs
DHS operates programs across components to execute against the variety of its cybersecurity missions. Below are a few such programs, but it is not an exhaustive list.

- The *National Cybersecurity Protection System (NCPS)* commonly referred to as *EINSTEIN* logs traffic coming into and out of agency networks from the public Internet, alerts when known malicious traffic is identified, and blocks certain malicious traffic. A limit of NCPS is that it has to have seen and analyzed the malicious traffic before, rather than being able to identify novel malicious traffic at first encounter—EINSTEIN can only block known threats.

- *Continuous Diagnostics and Mitigation (CDM)* is a program that deploys sensors on an agency's network to identify what the agency has attached to their network and the vulnerabilities of those devices. It compares this against intelligence to prioritize actively exploited vulnerabilities for patching.

- *Automated Information Sharing (AIS)* was authorized in the Cybersecurity Information Sharing Act of 2015 (P.L. 114-113 Division N, Title I) and provides for machine-to-machine sharing of cyber threat indicators and defensive measures among the private sector, to DHS, and through DHS, among federal agencies.

- *Electronic Crimes Task Forces (ECTF)* are operated by the USSS out of their field offices to assist local law enforcement in investigating computer crimes.

- The *Critical Infrastructure Cyber Community Voluntary Program (C^3VP)* seeks to encourage adoption of the NIST Cybersecurity Framework.

- The *National Cyber Security Alliance (NCSA)* is a public-private partnership between DHS and the private sector to promote cybersecurity awareness. National Cybersecurity Awareness Month is part of this partnership.

Working with Others for Cybersecurity
DHS serves a national customer base when delivering cybersecurity capabilities and developing policies. However, these customers may be divided into two main groups: the .gov domain and the .com domain—or, as described in the National Cybersecurity Protection Act of 2014, federal and non-federal entities. DHS has the power to compel federal agencies to act, but must collaborate and entice non-federal agencies to act.

Federal Agencies (.gov)
DHS has specific authorities with regard to federal agency cybersecurity. As such, DHS has established forums and coordination mechanisms to work with agencies to improve agency cybersecurity, and it has other mechanisms to work with agencies toward national cybersecurity. DHS must deploy security technologies on agency networks to improve the security of the .gov domain. In doing so, DHS has a process to obtain and maintain agreements with individual agencies for the use of that technology. DHS uses the federal chief information officer (CIO) and chief information security officer (CISO) councils, which discuss federal IT security broadly. DHS also collaborates with other agencies, like NIST and the DOE national laboratories, to develop and promulgate cybersecurity best practices for federal and non-federal entities.

Private Sector (.com)
DHS works with the IT sector to develop and implement improved cybersecurity tactics that could be deployed nationally. During the Obama Administration, policies were created to position DHS as the lead federal agency for interacting with the private sector on a variety of security matters. Presidential Policy Directive 41 (PPD-41) states that DHS is the lead for asset response, or helping victims of cyber attacks recover. This does not replace the FBI's responsibility for criminal investigation, as it states the FBI is the lead for threat response, nor does it detract from DOD's capabilities, as it is long-standing policy for military capabilities to supplement civilian capabilities when necessary as part of Defense Support for Civil Authorities (DSCA). Viewed another way, domestic cybersecurity is primarily a civilian matter rather than a military or law enforcement matter. However, the military and law enforcement agencies bring capabilities that can assist the private sector.

The Cybersecurity Act of 2015 establishes DHS as the portal for sharing information between the private sector and the government. DHS is obligated to inform other federal agencies of pertinent information without delay.

Chris Jaikaran, cjaikaran@crs.loc.gov, 7-0750

IF10683