Homeland Security

ENHANCED CYBERSECURITY SERVICES

ABOUT THE PROGRAM

The Department of Homeland Security's (DHS) Enhanced Cybersecurity Services (ECS) Program was expanded in February 2013 by Executive Order 13636: Improving Critical Infrastructure Cybersecurity as a voluntary information sharing program. ECS assists critical infrastructure owners and operators to improve protection of their systems from unauthorized access, exploitation, or data exfiltration.

ECS shares sensitive and classified government vetted cyber threat information with qualified Commercial Service Providers (CSPs) and Operational Implementers (OIs). In turn, the CSPs use the cyber threat information to protect their customers who are validated critical infrastructure entities. OIs use the cyber threat information to protect only their internal networks.

ECS augments, but does not replace entities' existing cybersecurity capabilities.

SERVICES (COUNTERMEASURES)

The ECS Program continues to consider and review additional services that can take advantage of the government vetted cyber threat indicators for use in enhancing the protection of our nation's critical infrastructure. Currently there are two (2) approved services* for use within the ECS Program:

1. DNS Sinkholing
2. E-mail Filtering

*Please refer to the ECS Privacy Impact Assessment (PIA) for more details at http://www.dhs.gov/cybersecurity-and-privacy.

ECS Information Sharing Protects the Nation!

> "The timeliness of the data was entirely appropriate, often included in the same day or next day after a report was issued. In the past few weeks there have been two zero day exploits released in the wild; pertinent indicators were included in the signatures."

For more information, please contact:
ECS_Program@hq.dhs.gov

CRITICAL INFRASTRUCTURE

ECS offers an enhanced approach to **protect** and **defend** critical infrastructure entities by supplementing existing commercial services and capabilities with U.S. Government cyber threat information. This approach supports the delivery of enhanced capabilities to validated participants from all critical infrastructure sectors.

Program participation is voluntary and is designed to protect government intelligence, corporate information security, and the privacy of participants, while enhancing the security of critical infrastructure.

DHS validates critical infrastructure entities from all critical infrastructure sectors that are then eligible to participate in the ECS program and receive ECS services from an eligible CSP.

Contact an eligible CSP to sign-up for ECS:
AT&T: ecs-pmo@list.att.com
CenturyLink: ecs@centurylink.com

COMMERCIAL SERVICE PROVIDERS & OPERATIONAL IMPLEMENTERS

In order to securely deliver ECS to our Nation's critical infrastructure, CSPs and OIs must meet eligibility requirements set forth by the ECS program and its partners. Once vetted, CSPs and OIs must enter into a Memorandum of Agreement (MOA) with DHS in order to participate in the program and receive government furnished threat indicators.

CSPs and OIs are responsible for funding and long-term maintenance of all sensitive and classified information in accordance with defined security requirements. CSPs and OIs implement services based on requirements designed to manage operational security concerns.

CSPs can deliver services to validated critical infrastructure entities through commercial relationships. The ECS program is not involved in establishing commercial relationships between CSPs and critical infrastructure entities.

ECS Information Sharing Protects the Nation!
For more information, please contact:
ECS_Program@hq.dhs.gov

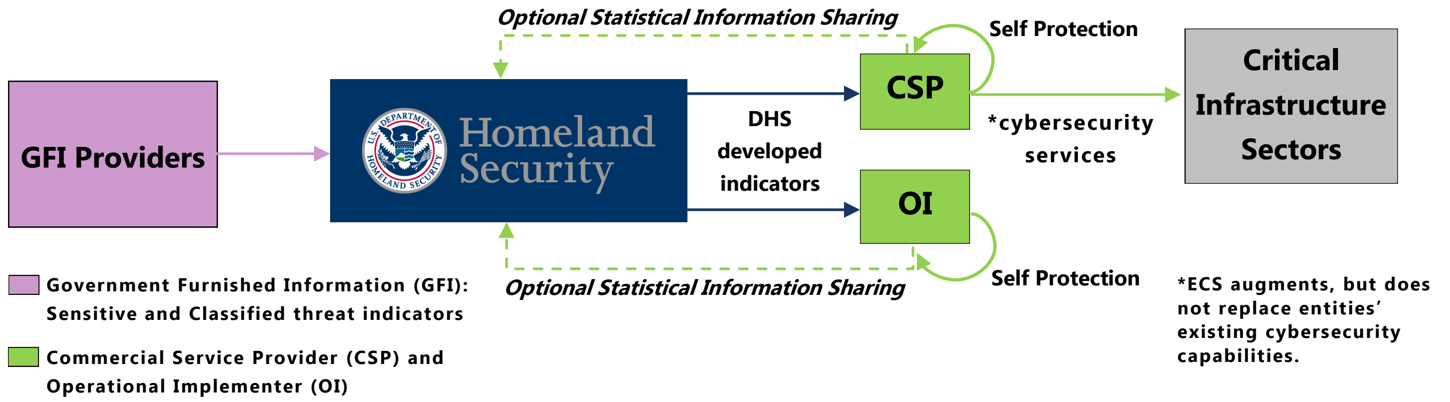
COMMITMENT TO PRIVACY

DHS remains strongly committed to preserving citizens' rights to privacy and the protection of civil liberties. DHS embeds and enforces privacy protections and transparency in all its activities and uses the Fair Information Practice Principles (FIPPs) to assess and mitigate any impact on an individual's privacy. ECS does not involve government monitoring of private networks or communications. DHS has conducted and published a Privacy Impact Assessment (PIA) for the ECS program. To read more about the FIPPs, the ECS PIA, and related programs, visit: **www.dhs.gov/privacy.**

ABOUT DHS CYBERSECURITY

DHS is responsible for safeguarding our Nation's critical infrastructure from physical and cyber threats that can affect national security, public safety, and economic prosperity. DHS actively engages the public and private sectors as well as international partners to prepare for, prevent, and respond to catastrophic incidents that could degrade or overwhelm these strategic assets. For more information, please visit: **www.dhs.gov/cyber**.

Enhanced Cybersecurity Services Program Model



🟪 Government Furnished Information (GFI): Sensitive and Classified threat indicators

🟩 Commercial Service Provider (CSP) and Operational Implementer (OI)

*ECS augments, but does not replace entities' existing cybersecurity capabilities.