Homeland Security

Office of Cybersecurity and Communications

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 - Improving Critical Infrastructure Cybersecurity.
- ECS is a voluntary information sharing program that assists critical infrastructure owners and operators to improve protection of their systems from unauthorized access, exploitation, or data exfiltration.
- ECS consists of the operational processes and security oversight required to share sensitive and classified cyber threat information with qualified Commercial Service Providers (CSPs) that will enable them to better protect their customers who are critical infrastructure entities.
- ECS augments, but does not replace, entities' existing cybersecurity capabilities. The ECS information sharing process protects CI entities against cyber threats that could otherwise harm their systems.
- DHS works with cybersecurity organizations from across the USG to gain access to a broad range of cyber threat information.
- The ECS program develops threat "indicators" with this information and provides CSPs with those indications of active, malicious cybersecurity activity.
- CSPs may use these threat indicators to provide approved cybersecurity services to critical infrastructure entities.

CRITICAL INFRASTRUCTURE ENTITIES

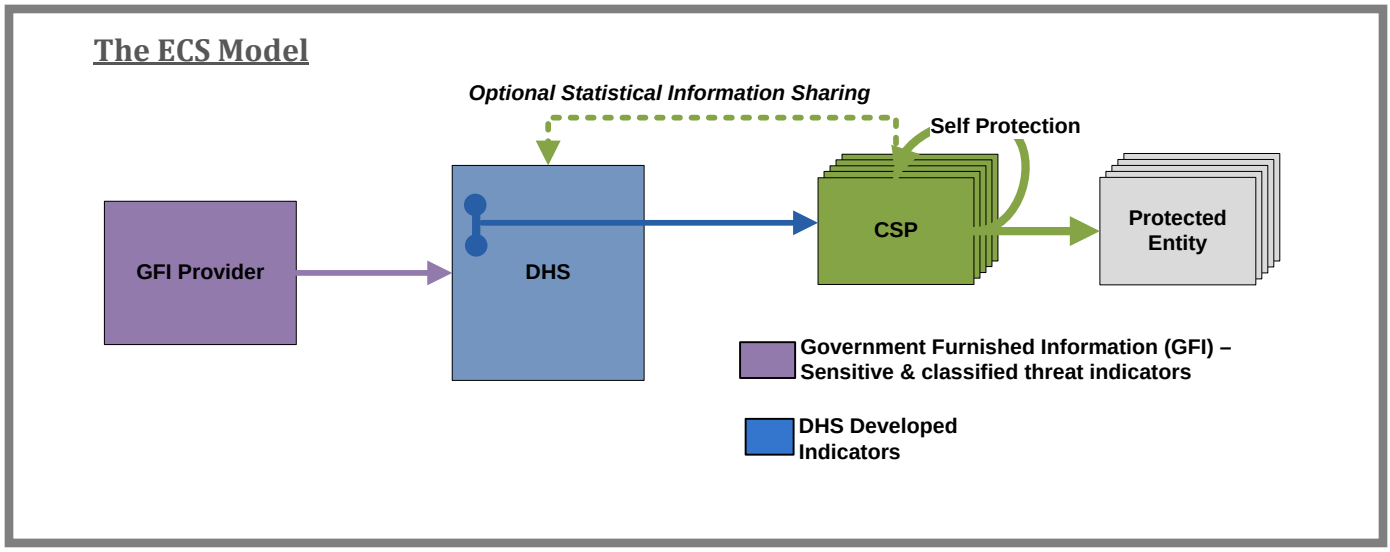
- Most CI entities already utilize cybersecurity services to protect their networks. ECS offers an enhanced approach to protect CI entities by supplementing existing services and commercial capabilities with USG threat information. This approach supports the delivery of enhanced capabilities to eligible participants from all sectors.
- Program participation is voluntary and designed to protect government intelligence, corporate information security, and the privacy of participants, while enhancing the security of critical infrastructure.
- Validated CI entities from all CI sectors are eligible to participate in the ECS program and receive ECS services from an eligible CSP.

Homeland Security

Office of Cybersecurity and Communications

COMMERCIAL SERVICE PROVIDERS

- In order to securely deliver ECS to our nation's critical infrastructure, CSPs must meet eligibility requirements set forth by the ECS program and its partners. Once vetted, CSPs must enter into a Memorandum of Agreement (MOA) with DHS in order to participate in the program and receive government furnished threat indicators.
- CSPs are responsible for handling, using, and maintaining all sensitive and classified information in accordance with defined security requirements. CSPs will only 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 CI entities.



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

Commitment to Privacy

DHS remains strongly committed to preserving citizens' right 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.