



# 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 helps U.S.-based public and private entities protect 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. OIs use the cyber threat information to protect only their internal networks.

### SERVICES (COUNTERMEASURES)

The ECS program continues to consider additional services that can use government-vetted cyber threat indicators to enhance the protection of U.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 augments, but does not replace entities' existing cybersecurity capabilities. For more information, please contact: [ECS\\_Program@hq.dhs.gov](mailto:ECS_Program@hq.dhs.gov)

### U.S.-BASED PUBLIC AND PRIVATE ENTITIES

ECS offers an enhanced approach to **protect** and **defend** U.S.-based public and private entities by supplementing

“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.”

existing commercial services and capabilities with U.S. Government cyber threat information. This approach supports the delivery of enhanced capabilities to participants located in the U.S.

Program participation is voluntary and is designed to protect government intelligence, corporate information security, and the privacy of participants, while enhancing the security of U.S.-based public and private entities.

### Contact an eligible CSP to sign-up for ECS:

AT&T: [ecs-pmo@list.att.com](mailto:ecs-pmo@list.att.com)

CenturyLink: [ecs@centurylink.com](mailto:ecs@centurylink.com)

Verizon: [vz-ecs@one.verizon.com](mailto:vz-ecs@one.verizon.com)

Lockheed Martin: [ecs.lm@lmco.com](mailto:ecs.lm@lmco.com)



# Homeland Security

## COMMERCIAL SERVICE PROVIDERS & OPERATIONAL IMPLEMENTERS

In order to securely deliver ECS to the Nation, 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 U.S.-based public and private entities through commercial relationships. The ECS program is not involved in establishing commercial relationships between CSPs and participating customers.

### ECS Information Sharing Protects the Nation!

For more information, please contact:

[ECS\\_Program@hq.dhs.gov](mailto: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](http://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](http://www.dhs.gov/cyber).

