



## ENHANCED CYBERSECURITY SERVICES

### PROGRAM OVERVIEW

The Department of Homeland Security's (DHS) Enhanced Cybersecurity Services (ECS) program is an intrusion prevention and analysis capability that helps U.S. based companies protect their computer systems against unauthorized access, exploitation, and data exfiltration. ECS works by sharing sensitive and classified cyber threat information with accredited Commercial Service Providers (CSPs). These CSPs in turn use that information to block certain types of malicious traffic from entering customer networks. ECS is meant to augment, but not replace, existing cybersecurity capabilities.

### SERVICE OFFERINGS

The ECS program currently offers three service offerings: **Domain Name Service (DNS) Sinkholing**, which blocks access to specified malicious domain names, **E-mail (SMTP) Filtering**, which blocks email with specified malicious criteria from entering a network, and **Netflow Analysis**, which uses passive detection to identify threats. The ECS program continues to consider additional services that can use government-vetted cyber threat indicators to enhance the protection of U.S. based organizations.

### PRIVACY

The ECS program embeds privacy and civil liberties protections into all of its operations. DHS ECS does not monitor any private networks or collect any communications, directly or by proxy. DHS uses the Fair Information Practice Principles to assess and mitigate individual privacy impacts. The ECS Privacy Impact Assessment determined that the U.S. Government and DHS do not collect any Personally Identifiable Information via ECS. To learn more about ECS Privacy, please visit: [www.dhs.gov/privacy](http://www.dhs.gov/privacy).

### ELIGIBILITY

All U.S.-based public and private entities are eligible to enroll in ECS. Program participation is voluntary and is designed to protect government intelligence, corporate



information security, and the privacy of participants. Four CSPs are accredited to provide ECS:

- **AT&T** ([ecs-pmo@list.att.com](mailto:ecs-pmo@list.att.com))
- **CenturyLink** ([ecs@centurylink.com](mailto:ecs@centurylink.com))
- **Lockheed Martin** ([ecs.lm@lmco.com](mailto:ecs.lm@lmco.com))
- **Verizon** ([vz-ecs@one.verizon.com](mailto:vz-ecs@one.verizon.com))

U.S.-based groups interested in participating or learning more about service-level options and agreements should contact an ECS CSP.

### ABOUT DHS CYBERSECURITY

DHS is responsible for safeguarding United States 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).

Please contact [ECS.Program@hq.dhs.gov](mailto:ECS.Program@hq.dhs.gov) with any program questions.