

Summary of the SECURE IT Act of 2013

The SECURE IT Act offers the right path forward to protect our nation from cyber threats, working towards true partnership between public and private sectors rather than imposing an additional prescriptive regulatory framework or creating new government bureaucracy.

SECURE IT is centered on consensus items and offers a balanced approach that will significantly advance our cybersecurity posture by focusing on five key areas:

Title I – Facilitating Sharing of Cyber Threat Information

- To help the private sector combat cyber threats and attacks, SECURE IT breaks down legal barriers in order to facilitate sharing of cyber-threat information among private sector entities and to and from the government and authorizes the private sector to use appropriate countermeasures against cyber threats.
- SECURE IT requires that a Federal agency be informed of a significant cyber incident involving its Federal information system. This provision will ensure that the government is privy to important information involving Federal information systems without mandatory requirements on privately owned and operated networks.
- SECURE IT includes a limited exemption from antitrust laws that currently restrict the exchange of information between private entities and provides full liability protection for the use and disclosure of cyber threat information, as authorized by the bill.
- SECURE IT does not modify or limit existing information sharing relationships or condition liability protections on an obligation to provide information to the Federal government, a condition that is likely to delay sharing at a time when rapid and flexible responses to evolving threats are a necessity. It does not foreclose direct sharing with any cybersecurity center.
- SECURE IT contains important and explicit protections for privacy and civil liberties, such as a precisely tailored definition of cyber threat information, consent provisions for use or disclosure, and opportunities for anonymization.
- SECURE IT also requires a comprehensive report to be prepared by the heads of each agency containing a cybersecurity center, in coordination with the Privacy and Civil Liberties Oversight Board, and directs a review by the Council of Inspectors General on Integrity and Efficiency.

Title II – Coordination of Federal Information Security Policy

- SECURE IT provides necessary reforms to the Federal Information Security Management Act (FISMA) to modernize the way the government manages and mitigates its own cyber risks. SECURE IT requires the implementation of an ongoing, automated threat assessment to maintain timely and actionable knowledge of the state of the security of Federal information systems. It also ensures that agencies will adopt and update technologies to detect and remediate cyber intrusions.

Title III – Criminal Penalties

- SECURE IT updates federal criminal statutes and streamlines existing, confusing penalties to facilitate the prosecution of cybercriminals. SECURE IT fills a void in existing Federal criminal law by establishing a criminal violation for aggravated damage to a critical infrastructure computer.

Title IV – Cybersecurity Research and Development:

- SECURE IT leverages existing Federal funding and programs to prioritize information technology and cybersecurity research and development. Research activities at the National Science Foundation and the National Institute of Standards and Technology will help the United States remain a leader in creating new innovative protections against cyber threats.

Title V – Data Security and Breach Notification:

- SECURE IT enhances information security by requiring entities take reasonable measures to protect and secure data in electronic form containing personal information.
- SECURE IT ensures covered entities notify individuals whose personal information is breached when it causes or is reasonably believed to have caused or will cause identity theft or financial harm.
- SECURE IT includes a federal preemptive standard for data security and breach notification, enforced by the Federal Trade Commission under Section 5 of the FTC Act, for covered entities.