



Committee on  
**HOMELAND SECURITY**  
Chairman Peter T. King

**SECTION BY SECTION ANALYSIS FOR THE  
PROMOTING AND ENHANCING CYBERSECURITY AND INFORMATION SHARING  
EFFECTIVENESS ACT OF 2011**

**Section 1 Short title**

The bill may be cited as the “Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act of 2011” or PrECISE Act.

**Section 2(a)** Subtitle C of the Homeland Security Act of 2002 is amended by adding:

**Section 226 National Cybersecurity Authority**

This section provides authority for the Secretary of Homeland Security to exercise its cybersecurity mission in protecting Federal networks and systems (defined as civilian, non-intelligence community networks and systems) and coordinating the protection of private sector critical infrastructure.

The Secretary is authorized to maintain the capability to act as the focal point for cybersecurity through technical expertise and policy development. The Secretary is required to coordinate cybersecurity activities across the Federal Government, designate a lead cybersecurity official within the Department of Homeland Security (DHS), publish a cybersecurity strategy and provide appropriate reports to Congress.

**Section 227 Identification of Sector Specific Cybersecurity Risks**

This section requires the Secretary, in conjunction with the heads of sector specific agencies, agencies with regulatory authority over critical infrastructure and the private sector, to identify and evaluate cybersecurity risks to each specific sector of critical infrastructure. The Secretary shall also review and collect existing performance standards and evaluate them against identified risks making this information available to the owners and operators of critical infrastructure. Agencies with regulatory authority over covered critical infrastructure would be required to incorporate the most effective and cost efficient standards into their existing regulatory regimes.

“Covered critical infrastructure” is defined as that infrastructure that if destroyed or disabled would result in a significant number of deaths, cause mass evacuations, major disruptions of the economy, or significant disruption to national security. The section provides for a redress procedure for facilities designated as covered critical infrastructure to appeal such designation.

**Section 228 Information Sharing**

The Secretary shall ensure that all threat information received in accordance with Section 202 of the Homeland Security Act of 2002 is provided to the National Information Sharing Organization (NISO) and in addition shall share relevant information regarding cyber threats and vulnerabilities with all federal agencies, state and local government representatives, and critical information infrastructure owners and operators. Information received from these agencies and operators will be designated Sensitive Security Information (SSI) and appropriately protected.

### **Section 229 Cybersecurity Research and Development**

The Under Secretary for Science and Technology shall support research and development designed to protect against acts of terrorism and cyber threats. Including work to improve and create technologies for detecting and containing attacks, and preventing future attacks. The Under Secretary shall coordinate activities with the Under Secretary for National Protection and Programs, the Assistant Secretary for Cybersecurity and Communications, and the Assistant Secretary for Infrastructure Protection, and the heads of other relevant Federal departments.

### **Section 230 Recruitment and Retention of Cybersecurity and Communications Employees**

The Secretary is authorized to designate Federal employees as members of the excepted service, and fix competitive compensation and retention bonuses for these positions.

### **Section 2(b) Clerical Amendments**

### **Section 2(c) Plan for Execution of Authorities**

The Secretary shall submit a report on how the Department will implement the new authorities granted to it in this section.

### **Section 3 National Information Security Organization**

The Homeland Security Act of 2002 is amended by adding the following:

#### **Section 241 Establishment of National Information Security Organization**

This section establishes a private not-for-profit organization to facilitate information sharing between the private sector and the Government. The board of directors, established by the Secretary, would designate an organization as the NISO based upon expressed criteria such as experience with information sharing and maximizing public/private partnerships.

#### **Section 242 Mission and Activities**

The NISO would have three major missions: first, facilitating the exchange of cyber threat information, best practices and technical assistance amongst its membership including the Government. Second, it would facilitate the creation of a common operating picture built from information contributed by technically sophisticated members such as the Government, Internet Service Providers, and other members with access to large amounts of network related information. Third, the NISO would act as a catalyst for cooperative research and development of member driven research projects. Additionally, the NISO would incorporate into its membership agreements for the transferability of intellectual property and integrate with the National Cybersecurity and Communications Integration Center at DHS.

#### **Section 243 Board of Directors**

The Board of Directors would be composed of representatives from five different Federal Government agencies including DHS and 13 members of the private sector. Those 13 members would be made up of 10 different critical infrastructure owners and operators, privacy and civil liberty experts, and the chair of the National Council of Information Sharing and Analysis Centers (ISACs). The Board would establish the charter for the organization, procedures for sharing information, and the criteria for membership. Additional sub-boards or technical advisory groups are authorized to assist the Board.

#### **Section 244 Charter**

The board shall develop a charter to govern the operations and administration of the NISO which shall address the following:

- (1) the organizational structure of the NISO;
- (2) the governance of the NISO;
- (3) the mission statement of the NISO;
- (4) criteria for membership and termination of such membership;
- (5) funding model for the NISO;
- (6) rules for sharing information, treatment of intellectual property rights, limitations on liability and considerations of measures needed to mitigate anti-trust concerns;
- (7) technical requirements for participation in the common operating picture;
- (8) rules for participating in collaborate research and development projects;
- (9) protections of privacy and civil liberties to be used by the NISO; and
- (10) security requirements for the protection of information

#### **Section 245 Membership**

The Board shall determine membership criteria for the NISO.

#### **Section 246 Funding**

Annual administrative and operational expenses for the NISO shall be paid by its members determined by the Board, although for the first three years of its existence there are authorized \$10 million per year in federal funding.

#### **Section 247 Classified Information**

The Director of the NISO shall facilitate the sharing of classified and de-classified information in the possession of a Federal agency related to threats to information networks with members of the NISO.

#### **Section 248 Voluntary Information Sharing**

Cybersecurity providers, entities that use cybersecurity providers, and those that protect themselves from cyber attacks are all able to voluntarily share cyber threat information with the NISO and its membership, including the Federal Government. That information is exempted from disclosure under the Freedom of Information Act (FOIA) and state disclosure laws; cannot be used in a lawsuit except with written consent of the entity submitting the information to the NISO; it shall not be used or disclosed for regulatory purposes. Providing the information to the Federal Government through the NISO shall relieve the submitter of any liability for failure to warn or failure to disclose.

The Board of the NISO will develop procedures for information sharing, and only information sharing in accordance with those procedures will be provided protections.

#### **Section 249 Annual Independent Audits**

The NISO shall have an independent audit on an annual basis that will review the compliance with the information sharing rules and procedures it is required to develop. That audit will be made available to the public and to Congress for review.

#### **Section 250 Penalties**

It shall be unlawful for any U.S. or Federal employees, officers or employees of the NISO or officers or employees of any NISO member, to disclose or make known any protected cyber threat information obtained in the course of the employee's official duties. Any person found violating this subsection shall be fined and/or imprisoned, and is subject to removal from employment.

#### **Section 251 Authority to Issue Warnings**

The Federal Government may issue advisories and warnings to any public or private entity or to the general public regarding threats to information networks. The government may not disclose the source of the submitted information, or any proprietary or generally private information.

#### **Section 252 Exemption from Antitrust Prohibitions**

The exchange of information between public sector members of the NISO shall not be considered a violation of any provision of antitrust laws.

#### **Section 253 Limitation**

For any year after fiscal year 2015 the amount authorized to be appropriated for the NISO may not exceed the amount provided by the largest private sector member of the NISO.

#### **Section 3(a)(2) Clerical Amendments**

#### **Section 3(b) Authorization of Appropriations for initial expenses.**