SECTION BY SECTION

H.R. 6066, the Cybersecurity Responsibility and Accountability Act of 2016

Introduced by Rep. Ralph Abraham and cosponsored by Chairman Lamar Smith

Sec. 1. Short Title
This section establishes the short title of the bill as the "Cybersecurity Responsibility and accountability Act of 2016."

Sec. 2. Definitions.
This section gives the term "major cybersecurity incident" the same meaning as the term "major incident" which is defined in OMB Memorandum M-16-03.

Sec. 3. Authority and Functions of the Director of NIST
This section further specifies the role of the Director of the National Institute of Standards and Technology (NIST) to develop and update cybersecurity standards and guidelines to fulfill the additional objectives and requirements of the Cybersecurity Responsibility and Accountability Act of 2016. This includes specifying the NIST Director's responsibilities relative to working with OMB and federal agency heads, conducting cybersecurity research to identify and address prevalent information security challenges, concerns, and knowledge gaps identified by agencies, and developing, publishing, and updating as necessary information security standards and guidelines for national security systems based on established standards and guidelines for information systems.

Sec. 4. Agency Heads.
This section holds agency heads accountable for their agencies by specifically assigning to them the responsibility of informing Congress about data breaches within their respective agency.

Sec. 5. Federal Agency Head Responsibilities.
This section directs OMB, NIST and DHS to develop the job description and responsibilities for an agency Chief Information Security Officer within 6 months of this Act's enactment.

This section also requires each agency to provide mandatory annual information security training and certification designed specifically for the agency head, which is to be developed and updated by NIST. The purpose of the training will be to ensure that the agency head has an understanding of federal cybersecurity policy, including an understanding of: the agency's information and information systems; potential impact of common types of cyber-attacks and data breaches on the agency's operations and assets; steps the agency head and employees should take to protect agency information and information systems, including not using private messaging system software or private e-mail servers for official communications; and annual FISMA reporting requirements.

This section also adds NIST as one of the agencies that will receive the annual report that agency heads send to OMB, DHS, GAO and various congressional committees, regarding the agency's adequacy and effectiveness of information security policies, procedures and practices.

This section also requires the annual agency report to include written certification by the agency head that NIST information security standards are being met by the agency. For any NIST standard

the agency does not meet, the agency head shall provide the reason for the failure, and include documentation by the OMB Director noting the agency's failure in meeting such standard.

Within six months after the enactment of this Act, this section also requires each agency head to develop a plan in consultation with the Comptroller General to implement all of the Comptroller General's recommendations regarding information security controls relevant to the agency. If there are any recommendations that an agency head does not meet, then the agency head shall provide the reasons for the failure to the OMB Director for the Director's approval. For each unimplemented recommendation, the plan shall include either the OMB Director's approval or certification by the Director of the agency head's failure to implement such recommendation.

Within six months after the enactment of this Act, this section also requires each agency head to develop a similar plan as described above with the agency's Inspector General (IG) relative to the IG's recommendations regarding the agency's information security program.

Sec 6. Annual Independent Evaluation.
This section modifies current law to distinguish between annual independent evaluations conducted by agency IGs of their agency's information security program and practices from independent evaluations of major cybersecurity incidents (further explained below).

Sec 7. Major Cybersecurity Incident Independent Evaluations.
This section requires an independent IG evaluation of each major cybersecurity incident experienced by the agency. The IG evaluation will provide a description of each incident including: the threats and threat actors; vulnerabilities and impacts; risk assessments conducted on the system before the incident; status of compliance of the affected information system with information security requirements at the time of the incident, including NIST information security standards and any information security control recommendations made by the agency's IG and the Comptroller General; and recommendations for research, process and policy actions the agency should consider taking to help prevent future similar incidents.

For major cybersecurity incidents involving breaches of personally identifiable information, the IG evaluation shall include: the number of individuals affected by the incident and a description of the information breached or exposed; an assessment of the risk of harm to affected individuals; and details of whether and when the agency notified affected individuals about the data breach and what protections were offered by the breached agency.

If the IG's evaluation of the major cybersecurity incident determines that the incident occurred because the agency head failed to comply sufficiently with the information security requirements, recommendations, or standards described above, the OMB Director shall, within 60 days of receiving the evaluation, take enforcement action. The action that the OMB Director may take includes recommending to the President the removal or demotion of the agency head, or ensuring the agency head does not receive any cash or pay awards or bonuses for a period of 1 year.

The OMB Director will provide to Congress a detailed explanation for any enforcement action taken or for any decision not to act.