AMENDMENT NO._____ Calendar No._____

Purpose: To ensure the appropriate disclosure of incidents related to government data.

IN THE SENATE OF THE UNITED STATES—112th Cong., 2d Sess.

S. 3414

To enhance the security and resiliency of the cyber and communications infrastructure of the United States.

Referred to the Committee on _____ and ordered to be printed

Ordered to lie on the table and to be printed

AMENDMENT intended to be proposed by Mr. WYDEN

Viz:

Beginning on page 46, strike line 6 and all that follows through page 57, line 3, and insert the following:

''(4) provide a mechanism to improve and continuously monitor the security of agency information security programs and systems, subject to the protection of the privacy of individual or customer-specific data, through a focus on continuous monitoring of agency information systems and streamlined reporting requirements rather than overly prescriptive manual reporting.

"SEC. 3552. DEFINITIONS.

"(a) IN GENERAL.—Except as provided under subsection (b), the definitions under section 3502 (including the definitions of the terms 'agency' and 'information system') shall apply to this subchapter.

"(b) OTHER TERMS.—In this subchapter:

"(1) ADEQUATE SECURITY.—The term 'adequate security' means security commensurate with the risk and impact resulting from the unauthorized access to or loss, misuse, destruction, or modification of information.

"(2) CONTINUOUS MONITORING.—The term 'continuous monitoring' means the ongoing real time or near real time process used to determine if the complete set of planned, required, and deployed security controls within an agency information system continue to be effective over time in light of rapidly changing information technology and threat development. To the maximum extent possible, subject to the protection of the privacy of individual or customer-specific data, this also requires automation of that process to enable cost effective, efficient, and consistent monitoring and provide a more dynamic view of the security state of those deployed controls.

"(3) COUNTERMEASURE.—The term 'countermeasure' means automated or manual actions with

defensive intent to modify or block data packets associated with electronic or wire communications, Internet traffic, program code, or other system traffic transiting to or from or stored on an information system for the purpose of protecting the information system from cybersecurity threats, conducted on an information system owned or operated by or on behalf of the party to be protected or operated by a private entity acting as a provider of electronic communication services, remote computing services, or cybersecurity services to the party to be protected.

''(4) INCIDENT.—The term 'incident' means an occurrence that—

''(A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of agency information or an agency information system; or

''(B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

''(5) INFORMATION SECURITY.—The term 'information security' means protecting agency information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

"(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring nonrepudiation and authenticity;

"(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

"(C) availability, which means ensuring timely and reliable access to and use of information.

"(6) INFORMATION TECHNOLOGY.—The term 'information technology' has the meaning given that term in section 11101 of title 40.

"(7) NATIONAL SECURITY SYSTEM.—

"(A) IN GENERAL.—The term 'national security system' means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

"(i) the function, operation, or use of which—

"(I) involves intelligence activities;

"(II) involves cryptologic activities related to national security;

"(III) involves command and control of military forces;

"(IV) involves equipment that is an integral part of a weapon or weapons system; or

"(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

"(ii) that is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

"(B) EXCLUSION.—Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

"(8) SECRETARY.—The term 'Secretary' means the Secretary of Homeland Security.

"SEC. 3553. FEDERAL INFORMATION SECURITY AUTHORITY AND COORDINATION.

"(a) IN GENERAL.—Except as provided in subsections (f) and (g), the Secretary shall oversee agency information security policies and practices, including the development and oversight of information security policies and directives and compliance with this subchapter.

"(b) DUTIES.—The Secretary shall—

"(1) develop, issue, and oversee the implementation of information security policies and directives, which shall be compulsory and binding on agencies to the extent determined appropriate by the Secretary, including—

"(A) policies and directives consistent with the standards promulgated under section 11331 of title 40 to identify and provide information security protections that are commensurate with the risk and impact resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

"(i) information collected, created, processed, stored, disseminated, or otherwise used or maintained by or on behalf of an agency; or

"(ii) information systems used or operated by an agency or by a contractor of

an agency or other organization, such as a State government entity, on behalf of an agency;

"(B) minimum operational requirements for network operations centers and security operations centers of agencies to facilitate the protection of and provide common situational awareness for all agency information and information systems;

"(C) reporting requirements, consistent with relevant law, regarding information security incidents;

"(D) requirements for agencywide information security programs, including continuous monitoring of agency information systems;

"(E) performance requirements and metrics for the security of agency information systems;

"(F) training requirements to ensure that agencies are able to fully and timely comply with directions issued by the Secretary under this subchapter;

"(G) training requirements regarding privacy, civil rights, civil liberties, and information

oversight for agency information security employees;

''(H) requirements for the annual reports to the Secretary under section 3554(c); and

''(I) any other information security requirements as determined by the Secretary;

''(2) review agency information security programs required to be developed under section 3554(b);

''(3) develop and conduct targeted risk assessments and operational evaluations for agency information and information systems in consultation with the heads of other agencies or governmental and private entities that own and operate such systems, that may include threat, vulnerability, and impact assessments and penetration testing;

''(4) operate consolidated intrusion detection, prevention, or other protective capabilities and use associated countermeasures for the purpose of protecting agency information and information systems from information security threats;

''(5) in conjunction with other agencies and the private sector, assess and foster the development of information security technologies and capabilities for use across multiple agencies;

''(6) designate an entity to receive reports and information about information security incidents, threats, and vulnerabilities affecting agency information systems;

''(7) provide incident detection, analysis, mitigation, and response information and remote or on-site technical assistance to the heads of agencies;

''(8) coordinate with appropriate agencies and officials to ensure, to the maximum extent feasible, that policies and directives issued under paragraph (1) are complementary with—

''(A) standards and guidelines developed for national security systems; and

''(B) policies and directives issues by the Secretary of Defense, Director of the Central Intelligence Agency, and Director of National Intelligence under subsection (g)(1);

''(9) not later than March 1 of each year, submit to Congress a report on agency compliance with the requirements of this subchapter, which shall include—

''(A) a summary of the incidents described by the reports required in section 3554(c);

''(B) a summary of the results of assessments required by section 3555;

"(C) a summary of the results of evaluations required by section 3556;

"(D) significant deficiencies in agency information security practices as identified in the reports, assessments, and evaluations referred to in subparagraphs (A), (B), and (C), or otherwise; and

"(E) planned remedial action to address any deficiencies identified under subparagraph (D); and

"(10) with respect to continuous monitoring reporting, allow operators of agency information systems to use processes that will protect the privacy of individual or non-government customer specific data.

"(c) ISSUING POLICIES AND DIRECTIVES.—When issuing policies and directives under subsection (b), the Secretary shall consider any applicable standards or guidelines developed by the National Institute of Standards and Technology and issued by the Secretary of Commerce under section 11331 of title 40. The Secretary shall consult with the Director of the National Institute of Standards and Technology when such policies and directives implement standards or guidelines developed by National Institute of Standards and Technology. To the maximum ex-

tent feasible, such standards and guidelines shall be complementary with standards and guidelines developed for national security systems.

''(d) COMMUNICATIONS AND SYSTEM TRAFFIC.—

''(1) IN GENERAL.—Notwithstanding any other provision of law, in carrying out the responsibilities under paragraphs (3) and (4) of subsection (b), if the Secretary makes a certification described in paragraph (2), the Secretary may acquire, intercept, retain, use, and disclose communications and other system traffic that are transiting to or from or stored on agency information systems and deploy countermeasures with regard to the communications and system traffic, unless the head of an agency determines within a reasonable time, and reports to the President, that such acquisition, interception, retention, use, or disclosure is contrary to the public interest and would seriously undermine important agency goals, activities, or programs.

''(2) CERTIFICATION.—A certification described in this paragraph is a certification by the Secretary that—

''(A) the acquisitions, interceptions, and countermeasures are reasonably necessary for

the purpose of protecting agency information systems from information security threats;

"(B) the content of communications will be collected and retained only when the communication is associated with a known or reasonably suspected information security threat, and communications and system traffic will not be subject to the operation of a countermeasure unless associated with the threats;

"(C) information obtained under activities authorized under this subsection will only be retained, used, or disclosed to protect agency information systems from information security threats, mitigate against such threats, or, with the approval of the Attorney General, for law enforcement purposes when—

"(i) the information is evidence of a cybersecurity crime that has been, is being, or is about to be committed; and