

1 **SEC. 406. FEDERAL COMPUTER SECURITY.**

2 (a) DEFINITIONS.—In this section:

3 (1) COVERED SYSTEM.—The term “covered sys-
4 tem” shall mean a national security system as de-
5 fined in section 11103 of title 40, United States
6 Code, or a Federal computer system that provides
7 access to personally identifiable information.

8 (2) COVERED AGENCY.—The term “covered
9 agency” means an agency that operates a covered
10 system.

11 (3) LOGICAL ACCESS CONTROL.—The term
12 “logical access control” means a process of granting
13 or denying specific requests to obtain and use infor-
14 mation and related information processing services.

15 (4) MULTI-FACTOR LOGICAL ACCESS CON-
16 TROLS.—The term “multi-factor logical access con-
17 trols” means a set of not less than 2 of the following
18 logical access controls:

19 (A) Information that is known to the user,
20 such as a password or personal identification
21 number.

22 (B) An access device that is provided to
23 the user, such as a cryptographic identification
24 device or token.

25 (C) A unique biometric characteristic of
26 the user.

1 (5) PRIVILEGED USER.—The term “privileged
2 user” means a user who, by virtue of function or se-
3 niority, has been allocated powers within a covered
4 system, which are significantly greater than those
5 available to the majority of users.

6 (b) INSPECTOR GENERAL REPORTS ON COVERED
7 SYSTEMS.—

8 (1) IN GENERAL.—Not later than 240 days
9 after the date of enactment of this Act, the Inspec-
10 tor General of each covered agency shall each submit
11 to each Comptroller General of the United States
12 and the appropriate committees of jurisdiction in the
13 Senate and the House of Representatives a report,
14 which shall include information collected from the
15 covered agency for the contents described in para-
16 graph (2) regarding the Federal computer systems
17 of the covered agency.

18 (2) CONTENTS.—The report submitted by each
19 Inspector General of a covered agency under para-
20 graph (1) shall include, with respect to the covered
21 agency, the following:

22 (A) A description of the logical access
23 standards used by the covered agency to access
24 a covered system, including—

1 (i) in aggregate, a list and description
2 of logical access controls used to access
3 such a covered system; and

4 (ii) whether the covered agency is
5 using multi-factor logical access controls to
6 access such a covered system.

7 (B) A description of the logical access con-
8 trols used by the covered agency to govern ac-
9 cess to covered systems by privileged users.

10 (C) If the covered agency does not use log-
11 ical access controls or multi-factor logical access
12 controls to access a covered system, a descrip-
13 tion of the reasons for not using such logical
14 access controls or multi-factor logical access
15 controls.

16 (D) A description of the following data se-
17 curity management practices used by the cov-
18 ered agency:

19 (i) The policies and procedures fol-
20 lowed to conduct inventories of the soft-
21 ware present on the covered systems of the
22 covered agency and the licenses associated
23 with such software.

1 (ii) What capabilities the covered
2 agency utilizes to monitor and detect
3 exfiltration and other threats, including—

4 (I) data loss prevention capabili-
5 ties; or

6 (II) digital rights management
7 capabilities.

8 (iii) A description of how the covered
9 agency is using the capabilities described
10 in clause (ii).

11 (iv) If the covered agency is not uti-
12 lizing capabilities described in clause (ii), a
13 description of the reasons for not utilizing
14 such capabilities.

15 (E) A description of the policies and proce-
16 dures of the covered agency with respect to en-
17 suring that entities, including contractors, that
18 provide services to the covered agency are im-
19 plementing the data security management prac-
20 tices described in subparagraph (D).

21 (3) EXISTING REVIEW.—The reports required
22 under this subsection may be based in whole or in
23 part on an audit, evaluation, or report relating to
24 programs or practices of the covered agency, and
25 may be submitted as part of another report, includ-

1 ing the report required under section 3555 of title
2 44, United States Code.

3 (4) CLASSIFIED INFORMATION.—Reports sub-
4 mitted under this subsection shall be in unclassified
5 form, but may include a classified annex.

6 (c) GAO ECONOMIC ANALYSIS AND REPORT ON FED-
7 ERAL COMPUTER SYSTEMS.—

8 (1) REPORT.—Not later than 1 year after the
9 date of enactment of this Act, the Comptroller Gen-
10 eral of the United States shall submit to Congress
11 a report examining, including an economic analysis
12 of, any impediments to agency use of effective secu-
13 rity software and security devices.

14 (2) CLASSIFIED INFORMATION.—A report sub-
15 mitted under this subsection shall be in unclassified
16 form, but may include a classified annex.

17 **SEC. 407. STRATEGY TO PROTECT CRITICAL INFRASTRUC-**
18 **TURE AT GREATEST RISK.**

19 (a) DEFINITIONS.—In this section:

20 (1) APPROPRIATE AGENCY.—The term “appro-
21 priate agency” means, with respect to a covered en-
22 tity—

23 (A) except as provided in subparagraph

24 (B), the applicable sector-specific agency; or

1 On page 91, line 11, strike “203 and 204” and insert
2 “303 and 304”.

3 On page 96, line 19, strike “likely,” and insert “like-
4 ly”.

5 On page 96, line 22, strike “present” and insert
6 “present,”.

7 On page 107, line 10, strike “shall each” and insert
8 “shall”.

9 On page 107, lines 11 and 12, strike “each Comp-
10 troller General of the United States and”.

11 On page 110, strikes lines 6 through 16.

12 On page 114, line 7, strike “SENATE” and insert
13 “SENSE”.