ЗАГОЛОВОК III - ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

СЕКЦИЯ 301. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ.

(a) СОКРАЩЕННОЕ НАЗВАНИЕ. - Этот заголовок может цитироваться как "Федеральный закон об управлении информационной безопасностью 2002".

(b) ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. -

(1) ВООБЩЕ. - Глава 35 заголовка 44, Кодекс Соединенных Штатов, исправлена путем добавления в конце следующего нового подраздела:

"ПОДРАЗДЕЛ III - ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

"§ 3541. Назначения

"Назначения этого подраздела -

"(1) служить всесторонней основой для того, чтобы гарантировать эффективность мер обеспечения информационной безопасности для информационных ресурсов, которые поддерживают федеральную деятельность и активы;

"(2) признать значительную сетевую природу текущего федерального вычислительного окружения и обеспечить эффективное обще-правительственное управление и надзор за соответствующими рисками информационной безопасности, включая координацию усилий по информационной безопасности всюду по гражданским лицам, национальной безопасности и сообществам обеспечения правопорядка;

"(3) предусмотреть разработку и поддержка минимальных мер безопасности, требуемых для защиты федеральной информации и информационных систем;

"(4) обеспечить механизм для улучшенного надзора за программами информационной безопасности Федеральных агентств;

"(5) подтвердить, что коммерчески разработанные продукты информационной безопасности предлагают продвинутые, динамичные, устойчивые и эффективные решения для информационной безопасности, отражая рыночные решения для защиты критических информационных инфраструктур, важных для национальной обороны и экономической безопасности страны, которые спроектированы, созданы и разработаны частным сектором; и

"(6) признать, что выбор конкретных технических аппаратных и программных решений для информационной безопасности из числа коммерчески разработанных продуктов должен быть оставлен конкретным агентствам.

"§ 3542. Определения

"(a) ВООБЩЕ. - За исключением представленных в подразделе (b), к этой подглаве должны применяться определения раздела 3502. *(см. в конце документа)*

"(b) ДОПОЛНИТЕЛЬНЫЕ ОПРЕДЕЛЕНИЯ. - использующиеся в этом подразделе:

"(1) термин 'информационная безопасность' означает защиту информации и информационных систем от несанкционированного доступа, использования, раскрытия, разрушения, модификации или разрушения, чтобы обеспечить -

"(A) целостность, что означает принятие мер против неподходящей модификации или разрушения информации и включает обеспечение неотказуемости и подлинности информации;

"(B) конфиденциальность, что означает сохранение установленных ограничений на доступ и раскрытие, включая средства для защиты персональной приватной и частной информации; и

"(C) доступность, что означает гарантирование своевременного и надежного доступа к и использование информации.

"(2) (A) термин 'система национальной безопасности' означает любую информационную систему (включая любую телекоммуникационную систему) используемую или применяемую агентством или подрядчиком агентства или другой организацией от имени агентства -

"(i) функция, деятельность, или использование которой -

"(I) включает разведывательную деятельность;

"(II) включает криптологические работы, связанные с национальной безопасностью;

"(III) включает командование и управление вооруженными силами;

"(IV) включает оборудование, которое является неотъемлемой частью оружия или систем оружия; или

"(V) предмет абзаца (B), является критической по отношению к прямому выполнению военных или разведывательных задач; или

"(ii) постоянно защищена процедурами, установленными для информации, которые были специально санкционированы согласно критериям, установленным Правительственным распоряжением или законом конгресса, чтобы сохраняться классифицированной в интересах национальной обороны или внешней политики.

"(B) Абзац (A) (i) (V) не включает системы, которые должны использоваться для стандартных административных и бизнес-приложений (включая заработную плату, финансы, логистику и приложения управления персоналом).

"(3) термин 'информационная технология' имеет значение данное этому термину в разделе 11101 из заголовка 40.

((6) Информационная технология. - Термин "информационная технология" - [1]

(A) в применении к средствам исполнительного агентства любое оборудование или взаимосвязанная система или подсистема оборудования, используемое в автоматическом получении, хранении, анализе, оценке, манипулировании, управлении, перемещении, контроле, демонстрации, переключении, обмене, передаче или приеме данных или информации исполнительным агентством, если оборудование используется исполнительным агентством непосредственно или используется подрядчиком в соответствии с контрактом с исполнительным агентством, который требует их -

(i) из этого оборудования; или

(ii) из этого оборудования до существенной степени в выполнении сервиса или оснащении продукта;

(B) включает компьютеры, вспомогательное оборудование (включая периферийные устройства отображения, устройства ввода, вывода и хранения, необходимые для безопасности и наблюдения), периферийное оборудование, разработанное, чтобы управляться центральным процессором компьютера, программное обеспечение, встроенное микропрограммное обеспечение и подобные процедуры, сервисы (включая сервисы поддержки) и связанные ресурсы; но

(C) не включает любое оборудование, получаемое федеральным подрядчиком эпизодически к федеральному контракту.)

"§ 3543. Полномочия и функции Директора *(Директор Министерства управления и бюджета)*

"(a) В ЦЕЛОМ. - Директор должен наблюдать за политиками и методами информационной безопасности агентств, включая -

"(1) разработку и наблюдение за реализацией политик, принципов, стандартов и руководств по информационной безопасности, включая посредством обеспечения агентствами своевременного принятия и соответствия со стандартами, провозглашенными в разделе 11331 из заголовка 40;

(Секция 11331. Обязанности по федеральным стандартам информационных систем

(a) Определение. - В этом разделе термин "информационная безопасность" имеет тоже значение, что и термин в разделе 3532 (b) (1) из заголовка 44.

(b) Требования по установлению стандартов. -

(1) В целом. -

(A) Требование. - За исключением обеспеченного в соответствии с абзацем (2), Директор Министерства управления и бюджета должен, на основе предложенных стандартов, разработанных Национальным институтом стандартов и технологий в соответствии с абзацами (2) и (3) из раздела 20 (a) закона о Национальном институте стандартов и технологий (15 конгрессов США 278g-3 (a)) и после консультаций с Секретарем национальной безопасности провозгласить стандарты информационной безопасности, имеющие отношение к федеральным информационным системам.

---

[1] Мелким курсивным текстом в документе приведены справочные материалы, вставленные при переводе для облегчения понимания основного текста.

(B) Требуемые стандарты. - Стандарты, провозглашенные под абзацем (A), должны включать -
(i) стандарты, которые обеспечивают минимальные требования информационной безопасности как определено в разделе 20 (b) закона о Национальном институте стандартов и технологий (15 U.S.C. 278g-3 (b)); и
(ii) такие стандарты, которые иначе необходимы, чтобы улучшить эффективность деятельности или безопасность федеральных информационных систем.
(C) Требуемое предназначение стандартов. - Стандарты Информационной безопасности, описанные под абзацем (B), должны быть обязательными и предписанными.
(2) Стандарты и руководства для систем национальной безопасности. -
Стандарты и руководства для систем национальной безопасности, как определено под разделом 3532 (3) из заголовка 44, должны быть разработаны, провозглашены, определены и наблюдаться как установлено законом и как предписано президентом.
(c) Применение более строгих стандартов. - Руководитель агентства может использовать стандарты для рентабельной информационной безопасности для всей деятельности и активов в пределах или под контролем этого агентства, которые являются более строгими, чем стандарты, провозглашенные Директором в этом разделе, если такие стандарты -
(1) содержат, как минимум, положения тех применимых стандартов, сделанных обязательными и предписанными Директором; и
(2) во всем остальном непротиворечивы с политиками и руководствами, выпущенными в соответствии с разделом 3533 из заголовка 44.
(d) Требования относительно решений Директора. -
(1) Крайний срок. - Решение относительно обнародования Директором любого стандарта из подраздела (b) должно произойти не позже 6 месяцев после представления Директору предложенного стандарта Национальным институтом стандартов и технологий, как предусмотрено в разделе 20 из закона о Национальном институте стандартов и технологий (15 U.S.C. 278g-3).
(2) Предложения и комментарии. - Решение Директора значительно изменить или не провозгласить стандарт, представленный Директору Национальным институтом стандартов и технологий, как предусмотрено в разделе 20 из закона о Национальном институте стандартов и технологий (15 U.S.C. 278g-3), должно быть принято после того, как обществу будет дана возможность прокомментировать решение, предложенное Директором.)

"(2) требования агентств, непротиворечивые со стандартами, провозглашенными в разделе 11331 и требованиями этого подраздела, чтобы идентифицировать и обеспечить защиту информационной безопасности, соразмерную с риском и величиной вреда, следующего из несанкционированного доступа, использования, раскрытия, разрушения, модификации или разрушения -

"(A) информации собираемой или сопровождаемой от имени агентства; или

"(B) информационных систем, которые используются или управляются агентством или подрядчиком агентства или другой организацией от имени агентства;

"(3) координирование разработки стандартов и руководств, указанных в разделе 20 из закона о Национальном институте стандартов и технологий (15 *U.S.C.* 278g-3) с агентствами и офисами эксплуатирующими или осуществляющими контроль над системами национальной безопасности (включая Агентство национальной безопасности), чтобы гарантировать до максимально выполнимой степени, что такие стандарты и руководства дополняют стандарты и руководства, разработанные для систем национальной безопасности;

"(4) наблюдение за соответствием агентств требованиям этого подраздела, включая посредством любого авторизованного действия в соответствии с разделом 11303 из заголовка 40, чтобы провести в жизнь подконтрольность для согласия с такими требованиями;

"(5) рассмотрение, по крайней мере ежегодно, и одобрение или не одобрение программ информационной безопасности агентств, требуемых в разделе 3544 (b);

"(6) координирование политик и процедур информационной безопасности с политиками и процедурами управления ресурсами соответствующей информации;

"(7) наблюдение за деятельностью федерального инцидентного центра информационной безопасности, требуемого в разделе 3546; и

"(8) создание отчетов к Конгрессу не позже чем 1 марта каждого года по соответствию агентств требованиям этого подраздела, включая -

"(A) сводку результатов оценок, требуемых в разделе 3545;

"(B) оценку разработки, обнародования, принятия и соответствия со стандартами, разработанными в соответствии с разделом 20 из закона о Национальном институте стандартов и технологий (15 *U.S.C.* 278g-3) и провозглашенными в разделе 11331 из заголовка 40;

"(C) существенные недостатки в методах информационной безопасности агентств;

"(D) планируемые восстановительные действия, чтобы устранить такие недостатки; и

"(E) сводку, по результатам рассмотрения Директором отчета, подготовленного Национальным институтом стандартов и технологий в соответствии с разделом 20 (d) (10) из закона о Национальном институте стандартов и технологий (15 *U.S.C.* 278g-3).

"(b) СИСТЕМЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ. - За исключением полномочий, описанных в абзацах (4) и (8) подраздела (a), полномочия Директора определенные этим разделом, не должны примениться к системам национальной безопасности.

"(c) СИСТЕМЫ МИНИСТЕРСТВА ОБОРОНЫ и ЦЕНТРАЛЬНОГО РАЗВЕДЫВАТЕЛЬНОГО УПРАВЛЕНИЯ США. - (1) полномочия Директора, описанные в абзацах (1) и (2) подраздела (a), должны быть делегированы Министру обороны в случае систем, описанных в абзаце (2) и Директору Центральной Разведки в случае систем, описанных в абзаце (3).

"(2) системы, описанные в этом абзаце, являются системами, которыми управляют Министерство обороны, подрядчик Министерства обороны или другая сущность от имени Министерства обороны, которые обрабатывают любую информацию несанкционированный доступ, использование, раскрытие, разрушение, модификация или разрушение которой оказало бы ослабляющее влияние на предназначение Министерства обороны.

"(3) системы, описанные в этом абзаце, являются системами, которыми управляют Центральное разведывательное управление США, подрядчик Центрального разведывательного управления США, или другая сущность от имени Центрального разведывательного управления США, которые обрабатывают любую информацию несанкционированный доступ, использование, раскрытие, разрушение, модификация или разрушение которой оказало бы ослабляющее влияние на предназначение Центрального разведывательного управления США.

''§ 3544. Обязанности федерального агентства

"(a) ВООБЩЕ. - Руководитель каждого агентства должен -

"(1) быть ответственным за -

"(A) обеспечение защиты информационной безопасности, соразмерной с риском и величиной вреда, следующего из несанкционированного доступа, использования, раскрытия, разрушения, модификации или уничтожения -

"(i) информации собираемой или сопровождаемой от имени агентства; и

"(ii) информационных систем, которые используются или управляются агентством или подрядчиком агентства или другой организации от имени агентства;

"(B) исполнение требований этого подраздела и связанных политик, процедур, стандартов и руководств, включая -

"(i) стандарты информационной безопасности, провозглашенные в разделе 11331 из заголовка 40; и

"(ii) стандарты информационной безопасности и руководства для систем национальной безопасности, выпущенные в соответствии с законом и как предписано Президентом; и

"(C) гарантирование, что процессы управления информационной безопасностью интегрированы в стратегические и оперативные процессы планирования агентства;

"(2) гарантировать, что старшие должностные лица агентства обеспечивают информационную безопасность для информации и информационных систем, которые поддерживают деятельность и активы, находящиеся под их контролем, включая через -

"(A) оценку риска и величины вреда, который может следовать из несанкционированного доступа, использования, раскрытия, разрушения, модификации или разрушения такой информации или информационных систем;

"(B) определение уровней информационной безопасности необходимых, чтобы защитить такую информацию и информационные системы в соответствии со стандартами, провозглашенными в разделе 11331 из заголовка 40, для классификации информационной

безопасности и связанных требований;

"(C) реализацию политик и процедур, чтобы рентабельно уменьшить риски до допустимого уровня; и

"(D) периодическое тестирование и оценивание мер и технологий информационной безопасности, чтобы гарантировать, что они эффективно реализованы;

"(3) делегировать Директору по информации агентства, установленному в разделе 3506 (или сопоставимое должностное лицо в агентстве, нет охваченное этим разделом) полномочий, чтобы гарантировать согласие требованиями, наложенными на агентство в этой подглаве, включая -

"(A) назначение старшего менеджера по информационной безопасности агентства, который должен -

"(i) выполнять обязанности Директора по информации в соответствии с этим разделом;

"(ii) обладать профессиональной квалификацией, включая обучение и опыт, требуемой, чтобы управлять функциями, описанными в этом разделе;

"(iii) иметь режим работы по информационной безопасности как основной режим работы этого должностного лица; и

"(iv) возглавлять офис с задачей и ресурсами, необходимыми, чтобы помочь в обеспечении согласия агентства с этим разделом;

"(B) разработку и поддержание программы информационной безопасности всего агентства как требуется подразделом (b);

"(C) развитие и сопровождение политики информационной безопасности, процедур и технологий контроля, чтобы выполнить все применимые требования, включая выпущенных в соответствии с разделом 3543 из этого заголовка и разделом 11331 из заголовка 40;

"(D) обучение и наблюдение за персоналом с существенными обязанностями по информационной безопасности относительно таких обязанностей; и

"(E) помощь старшим должностным лицам агентства относительно их обязанностей в соответствии с абзацем (2);

"(4) гарантировать, что агентство обучило персонал, достаточный, чтобы помочь агентству в исполнении требований этого подраздела и связанных политик, процедур, стандартов и руководств; и

"(5) гарантировать, что Директор по информации агентства в координации с другими старшими должностными лицами агентства, отчитывается ежегодно руководителю агентства о эффективности программы информационной безопасности агентства, включая прогресс восстановительных действий.

"(b) ПРОГРАММА АГЕНТСТВА. - Каждое агентство должно разработать, задокументировать и реализовать программу информационной безопасности всего агентства, одобренную Директором в соответствии с разделом 3543 (a) (5), чтобы обеспечить информационную безопасность для информации и информационных систем, которые поддерживают деятельность и активы агентства, включая обеспеченные или управляемые другим агентством, подрядчиком или другим источником, которая включает -

"(1) периодические оценки риска и величина вреда, который может следовать из несанкционированного доступа, использования, раскрытия, разрушения, модификации или разрушения информации и информационных систем, которые поддерживают деятельность и активы агентства;

"(2) политики и процедуры, которые -

"(A) основаны на оценках степени риска, требуемых абзацем (1);

"(B) рентабельно уменьшают риски информационной безопасности до допустимого уровня;

"(C) гарантируют, что информационная безопасность обеспечивается всюду по жизненному циклу каждой информационной системы агентства; и

"(D) гарантируют согласие -

"(i) с требованиями этого подраздела;

"(ii) политикам и процедурам, которые предписаны Директором, и стандартами информационной безопасности, провозглашенными в разделе 11331 из заголовка 40;

"(iii) с минимально приемлемыми системными требованиям конфигурации, как

определено агентством; и

"(iv) с любыми другими применимыми требованиями, включая стандарты и руководства для систем национальной безопасности, выпущенными в соответствии с законом и как предписано Президентом;

"(3) иерархию планов обеспечения адекватной безопасности информации для сетей, средств и систем или групп информационных систем соответственно;

"(4) обучение по освоению безопасности, чтобы доводить до персонала, включая подрядчиков и других пользователей информационных систем, которые поддерживают деятельность и активы агентства, -

"(A) риски информационной безопасности связанные с их работами; и

"(B) их обязанности по исполнению политик и процедур агентства, разработанных, чтобы уменьшить эти риски;

"(5) периодическое тестирование и оценку эффективности политик информационной безопасности, процедур и методов, которое должно выполняться с частотой в зависимости от риска, но не реже, чем ежегодно, при этом тестирование -

"(A) должно включать тестирование организационных, эксплуатационных и технических мер каждой информационной системы, идентифицированной в реестре, требуемом в разделе 3505 (c); и

"(B) может включать тестирование, предусмотренное в оценке в разделе 3545;

"(6) процессы планирования, реализации, оценки и документирования восстановительных действий, чтобы устранять любые недостатки в политиках информационной безопасности, процедурах и методах агентства;

"(7) процедуры для того, чтобы обнаруживать, сообщать и реагировать на инциденты безопасности, непротиворечивые со стандартами и руководствами, выпущенными в соответствии с разделом 3546 (b), включая -

"(A) смягчение рисков, связанных с такими инцидентами, прежде чем будет нанесен существенный ущерб;

"(B) уведомление и консультация с федеральным инцидентным центром по информационной безопасности, упомянутым в разделе 3546; и

"(C) уведомление и консультация с, как соответственно -

"(i) правоохранительными органами и соответствующими Офисами Генерального инспектора;

"(ii) офисом, определяемый Президентом для каждого инцидента, затрагивающего системы национальной безопасности; и

"(iii) любым другим агентством или офисом в соответствии с законом или как предписано Президентом; и

"(8) планы и процедуры, чтобы гарантировать непрерывность деятельности для информационных систем, которые поддерживают деятельность и активы агентства.

"(c) СОЗДАНИЕ ОТЧЕТОВ АГЕНТСТВА. - Каждое агентство должно -

"(1) отчитываться ежегодно Директору, Комитетам по Правительственной Реформе и Науке Палаты представителей, Комитетам по Правительственным Делам и Торговле, Науке и Перевозкам Сената, соответствующим установленным и ассигнованным комитетам Конгресса и Генеральному контролеру по соответствию и эффективности политик информационной безопасности, процедур и методов, и согласия с требованиями этого подраздела, включая согласие с каждым требованием подраздела (b);

"(2) указывать соответствие и эффективность политик информационной безопасности, процедур и методов в планах и отчетах, касающихся

"(A) ежегодных бюджетов агентства;

"(B) управления ресурсами информации в соответствии с подразделом 1 из этой главы;

"(C) управления информационными технологиями в соответствии с подзаголовком III из заголовка 40;

"(D) результативности программы в соответствии с разделами 1105 и 1115 - 1119 заголовка 31, и разделами 2801 и 2805 из заголовка 39;

"(E) финансового менеджмента в соответствии с главой 9 заголовка 31 и законом Финансовых директоров 1990 (31 конгресс США 501 примечание; Общественным законом 101-576) (и поправками, внесенными тем законом);

"(F) системы финансового менеджмента согласно федеральному закону об Улучшении Финансового менеджмента (31 *U.S.C.* 3512 примечаний); и

"(G) внутреннего бухгалтерского учета и административного контроля в соответствии с разделом 3512 из заголовка 31, (известным как «Закон Федеральных менеджерах Финансовой Целостности»); и

"(3) сообщать о любом существенном недостатке в политике, процедуре или практике, идентифицированном в соответствии с абзацем (1) или (2) -

"(A) как материальный недостаток в отчете, создаваемом в соответствии с разделом 3512 из заголовка 31; и

"(B) если касается системы финансового менеджмента, как случай нехватки существенного соответствия федеральному закону об Улучшении Финансового менеджмента (31 *U.S.C.* 3512, примечание).

"(d) ИСПОЛНИТЕЛЬНЫЙ ПЛАН. - (1) В дополнение к требованиям подраздела (c), каждое агентство, после консультаций с Директором, должно включать как часть исполнительного плана, требуемого в разделе 1115 заголовка 31 описание -

"(A) периодов времени, и

"(B) ресурсов, включая бюджет, укомплектование и обучение, которые необходимы, чтобы реализовать программу, требуемую в подразделе (b).

"(2) описание в соответствии с абзацем (1) должно быть основано на оценке степени риска, требуемой в подразделе (b) (2) (1).

"(e) УВЕДОМЛЕНИЕ ОБЩЕСТВА и КОММЕНТАРИИ. - Каждое агентство должно предоставить обществу своевременное уведомление и возможности для комментариев к предложенным политикам информационной безопасности и процедурам до такой степени, насколько такие политики и процедуры влияют на взаимодействие с обществом.

"§ 3545. Ежегодная независимая оценка

"(a) В ЦЕЛОМ. - (1) Каждый год каждое агентство должно выполнять независимую оценку программы и практики информационной безопасности агентства, чтобы определить эффективность такой программы и практики.

"(2) Каждая оценка в соответствии с этим разделом должна включать -

"(A) тестирование эффективности политик, процедур и методов информационной безопасности представительного подмножества информационных систем агентства;

"(B) оценку (сделанную на основе результатов тестирования) согласия с -

"(i) требованиями этого подраздела; и

"(ii) соответствующей политикой, процедурами, стандартами и руководствами по безопасности информации; и

"(C) отдельное представление, где соответствующе, относительно информационной безопасности, касающейся систем национальной безопасности.

"(b) НЕЗАВИСИМЫЙ АУДИТОР. - Согласно подразделу (c) -

"(1) для каждого агентства с Генеральным инспектором, назначенным согласно закону о Генеральном инспекторе от 1978г., Генеральным инспектором или независимым внешним аудитором должна быть выполнена ежегодная оценка, требуемая в этом разделе, как определено Генеральным инспектором агентства; и

"(2) для каждого агентства, к которому не применим абзац (1), руководитель агентства должен

нанять независимого внешнего аудитора, чтобы выполнить оценку.

"(c) СИСТЕМЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ. - Для каждого агентства эксплуатирующего или осуществляющего контроль над системой национальной безопасности та часть оценки, которая требуется этим разделом, непосредственно касающаяся системы национальной безопасности, должна быть выполнена–

"(1) только сущностью, определяемой руководителем агентства; и

"(2) в таком способе, чтобы обеспечить соответствующую защиту для информации связанной с любой уязвимостью информационной безопасности в такой системе, соразмерной с риском и в соответствии со всеми действующими законами.

"(d) ОСУЩЕСТВЛЕНИЕ ОЦЕНКИ. - Оценка, требуемая в этом разделе может базироваться полностью или частично на аудите, оценке или отчете, соответствующим программам или практикам, применяемым агентством.

"(e) СОЗДАНИЕ ОТЧЕТОВ АГЕНТСТВА. - (1) Каждый год, не позже даты, установленной Директором, руководитель каждого агентства должен представить Директору результаты оценки, требуемой в этом разделе.

"(2) До степени оценки, требуемой в этом разделе, непосредственно касающейся системы национальной безопасности, результаты оценки, представленные Директору, должны содержать только сводку и результтаты той части оценки, которая непосредственно касается системы национальной безопасности.

"(f) ЗАЩИТА ИНФОРМАЦИИ. - Агентства и оценщики должны сделать соответствующие шаги, чтобы обеспечить защиту информации, которая, если будет раскрыта, может оказать негативное влияние на информационную безопасность. Такая защита должна быть соразмерна с риском и соответствовать всем действующим законам и нормативным документам.

"(g) ОТЧЕТЫ OMB КОНГРЕССУ. - (1) Директор должен суммировать результаты оценок, проведенных в соответствии с этим разделом в отчете к Конгрессу, требуемому в разделе 3543 (a) (8).

"(2) Отчет Директора к Конгрессу в соответствии с этим подразделом должен суммировать информацию относительно информационной безопасности, касающейся систем национальной безопасности в таком способе, чтобы обеспечить соответствующую защиту для информации, связанной с любой уязвимостью информационной безопасности в такой системе, соразмерной с риском и в соответствии со всеми действующими законами.

"(3) Оценки и любые другие описания информационных систем под полномочиями и контролем Директора Центрального разведывательного управления или систем Национальных Внешних Разведывательных Программ под полномочиями и контролем Министра обороны должны быть сделаны доступными для Конгресса только через соответствующие комитеты по надзору Конгресса в соответствии с действующими законами.

"(h) ГЕНЕРАЛЬНЫЙ КОНТРОЛЕР. - Генеральный контролер должен периодически оценивать и отчитываться Конгрессу по -

"(1) соответствию и эффективности политик и практики информационной безопасности агентства; и

"(2) реализации требований этого подраздела.

''§ 3546. Федеральный инцидентный центр по информационной безопасности

"(a) В ЦЕЛОМ. - Директор должен гарантировать деятельность центрального Федерального инцидентного центра по информационной безопасности по -

"(1) предоставлению своевременной технической помощи операторам информационных систем агентств относительно инцидентов безопасности, включая руководство по обнаружению и обработке инцидентов информационной безопасности;

"(2) обобщению и анализу информации об инцидентах, которые угрожают информационной безопасности;

"(3) сообщению операторам информационных систем агентств о текущих и потенциальных угрозах и уязвимостях информационной безопасности; и

"(4) консультированию совместно с Национальным институтом стандартов и технологий, агентств или офисов, эксплуатирующий или осуществляющий контроль над системами национальной безопасности (включая Агентство национальной безопасности), и других таких агентств или офисов в соответствии с законом и как предписано Президентом относительно инцидентов информационной безопасности и связанных вопросов.

"(b) СИСТЕМЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ. - Каждое агентство, эксплуатирующее или осуществляющее контроль над системой национальной безопасности, должно делиться информацией об инцидентах информационной безопасности, угрозах и уязвимостях с федеральным инцидентным центром по информационной безопасностью до степени, непротиворечивой со стандартами и руководствами для систем национальной безопасности, выпущенными в соответствии с законом и как предписано Президентом.

''§ 3547. Системы национальной безопасности

"Руководитель каждого агентства, эксплуатирующего или осуществляющего контроль над системой национальной безопасности, должен быть ответственным за обеспечение того, что агентство -

"(1) обеспечивает защиту информационной безопасности, соразмерную с риском и величиной вреда, следующего из несанкционированного доступа, использования, раскрытия, разрушения, модификации или уничтожения информации, содержавшейся в такой системе;

"(2) реализует политику и практику информационной безопасности как требуется по стандартам и руководствам для систем национальной безопасности, выпущенным в соответствии с законом и как предписано Президентом; и

"(3) выполняет требования этого подраздела.

''§ 3548. Санкционирование ассигнований

"Должны быть санкционированы ассигнования таких сумм, которые могут быть необходимыми в каждом из бюджетных лет с 2003 по 2007, чтобы выполнить положения этого подраздела.

''§ 3549. Влияние на существующее законодательство

"Ничто в этом подразделе, разделе 11331 из заголовка 40, или разделе 20 из закона о Национальном Институте Стандартов Технологий (15 U.S.C. 278g-3) не может быть рассмотрено, как влияние на полномочия Президента, Министерства управления и бюджета или его Директора, Национального института стандартов и технологий или руководителя какого либо агентства, относительно санкционированного использования или разглашения информации, включая относительно защиты неприкосновенности частной жизни в соответствии с разделом 552a заголовка 5, разглашения информации в соответствии с разделом 552 из заголовка 5, управления и размещения документов в соответствии с главами 29, 31, или 33 из заголовка 44, управления ресурсами информации в соответствии с подразделом I из главы 35 этого заголовка, или разглашение информации Конгрессу или Генеральному контролеру Соединенных Штатов. Пока этот подраздел действует, подраздел II из этой главы не должен применяться.".

СЕКЦИЯ 302. УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ ТЕХНОЛОГИЯМИ.

(a) В ЦЕЛОМ. - раздел 11331 из заголовка 40, кодекса Соединенных Штатов, исправлен, чтобы читать следующим образом:

''§ 11331. Обязанности по стандартам федеральных информационных систем

"(a) СТАНДАРТЫ и РУКОВОДСТВА. -

"(1) Полномочия по предписанию. - За исключением установленного в соответствии с абзацем (2), Министр торговли должен, на основе стандартов и руководств, разработанных Национальным институтом стандартов и технологий в соответствии с абзацами (2) и (3) раздела 20 (a) закона о Национальном институте стандартов и технологий (15 U.S.C. 278g-3 (a)), предписывать стандарты и руководства, имеющие отношение к федеральным информационным системам.

"(2) СИСТЕМЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ. - Стандарты и руководящие указания для систем национальной безопасности (как определенно в этом разделе) должны быть разработаны, предписаны, определены и наблюдаться так, как иначе санкционировано законом и как предписано Президентом.

"(b) ОБЯЗАТЕЛЬНЫЕ ТРЕБОВАНИЯ. -

"(1) Полномочия по обязательности. - За исключением обеспеченного в соответствии с абзацем (2), Министр должен сделать стандарты предписанные в подразделе (a) (1) обязательными и предписанными до степени, которую определит необходимой Министр, чтобы улучшить эффективность деятельности или безопасность федеральных информационных систем.

"(2) ТРЕБУЕМЫЕ ОБЯЗАТЕЛЬНЫЕ СТАНДАРТЫ. - (A) Стандарты, предписанные в подразделе (a) (1), будут включать стандарты информационной безопасности -

"(i) обеспечивающие минимальные требования информационной безопасности как определено в разделе 20 (b) закона о Национальном институте стандартов и технологий (15 U.S.C. 278g-3 (b)); и

"(ii) иначе необходимые, чтобы улучшить безопасность федеральной информации и информационных систем.

"(B) стандарты Информационной безопасности, описанные в абзаце, (A) должен быть обязательным и предписанными.

"(c) Полномочия по не одобрению или изменению. - Президент может не одобрить или изменить стандарты и руководства, упомянутые в подразделе (a) (1), если Президент определяет что такое действие в интересах общества. Президентские полномочия, чтобы не одобрить или изменить такие стандарты и руководства не могут быть делегированы. Уведомление о таком неодобрении или модификации должно быть быстро опубликовано в Федеральном реестре. Получив уведомление о таком неодобрении или модификации, Министр торговли должен сразу отменить или изменить такие стандарты или руководства как предписано Президентом.

"(d) ИСПОЛЬЗОВАНИЕ ПОЛНОМОЧИЙ. - Чтобы гарантировать согласованность финансов и политики, Министр должен использовать полномочия, предусмотренные этим разделом в соответствии с предписанием Президента и в координации с Директором Министерства управления и бюджета.

"(e) ПРИЛОЖЕНИЕ БОЛЕЕ СТРОГИХ СТАНДАРТОВ. - Руководитель исполнительного агентства может использовать стандарты для рентабельной информационной безопасности для информационных систем в пределах или при контроле тем агентством, которые являются более строгими чем стандарты, которые Министр предписывает в соответствии с этим разделом если более строгие стандарты -

"(1) содержат, по крайней мере, применимые стандарты, сделанные обязательными и предписанными Министром; и

"(2) иначе непротиворечивы с политиками и руководствами, выпущенными в соответствии с разделом 3543 из заголовка 44.

"(f) РЕШЕНИЯ ОБ ОБНАРОДОВАНИИ СТАНДАРТОВ. - Решение Министра относительно обнародования любого стандарта в соответствии с этим разделом должно произойти не позже 6 месяцев после представления предложенного Министру стандарта Национальным институтом стандартов и технологий, как предусмотрено в разделе 20 из закона о Национальном институте стандартов и технологий (15 U.S.C. 278g-3).

"(g) ОПРЕДЕЛЕНИЯ. - в этом разделе:

"(1) ФЕДЕРАЛЬНАЯ ИНФОРМАЦИОННАЯ СИСТЕМА. - термин 'федеральная информационная система' означает информационную систему, которая используется или управляется исполнительным агентством, подрядчиком исполнительного агентства или другой организацией от имени исполнительного агентства.

"(2) ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. - термин 'информационная безопасность' соответствует термину в разделе 3542 (b) (1) из заголовка 44.

"(3) СИСТЕМА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ. - термин 'система национальной безопасности' соответствует термину в разделе 3542 (b) (2) из заголовка 44.".

СЕКЦИЯ 303. НАЦИОНАЛЬНЫЙ ИНСТИТУТ СТАНДАРТОВ И ТЕХНОЛОГИЙ.

Раздел 20 из закона о Национальном институте стандартов и технологий (15 U.S.C. 278g-3), исправлен, исключая текст и вставляя следующее:

"(a) В ЦЕЛОМ. - Институт должен -

"(1) иметь задачу развития стандартов, руководств и связанных методов и технологий для информационных систем;

"(2) разрабатывать стандарты и руководства, включая минимальные требования, для информационных систем, которые используют или управляют агентства или подрядчики агентств или другие организации от имени агентств, кроме систем национальной безопасности (как определено в разделе 3542 (b) (2) из заголовка 44, кодекса Соединенных Штатов); и

"(3) разрабатывать стандарты и руководства, включая минимальные требования, для того, чтобы обеспечить соответствующую безопасность информации и активов для всей деятельности агентств, но такие стандарты и руководящие указания - не должны применяться к системам национальной безопасности.

"(b) МИНИМАЛЬНЫЕ ТРЕБОВАНИЯ ДЛЯ СТАНДАРТОВ И РУКОВОДСТВ. - Стандарты и руководства, требованные подразделом (a), должны включать, как минимум

"(1) (A) стандарты, которые будут использоваться всеми агентствами, чтобы категорировать всю информацию и информационные системы, принадлежащие или сопровождаемые непосредственно или от имени каждого агентства, основанные на целях обеспечения соответствующих уровней информационной безопасности согласно масштабу уровней риска;

"(B) руководства, рекомендующие типы информации и информационные системы, которые должны быть включены в каждую такую категорию; и

"(C) минимальные требования информационной безопасности для информации и информационных систем для каждой такой категории;

"(2) определение и руководства по обнаружению и обработке инцидентов информационной безопасности; и

"(3) руководства, разрабатываемые совместно с Министерством обороны, включая Агентство национальной безопасности, для того, чтобы идентифицировать информационную систему как систему национальной безопасности, непротиворечивую с применимыми требованиями для систем национальной безопасности, выпущенных в соответствии с законом и как предписано Президентом.

"(c) РАЗРАБОТКА СТАНДАРТОВ И РУКОВОДСТВ. - При разработке стандартов и руководств, требуемых подразделами (a) и (b), Институт должен -

"(1) консультироваться с другими агентствами и офисами и частным сектором (включая Директора Министерства управления и бюджета, Министерств обороны и энергетики, Агентства национальной безопасности, Главного бюджетно-контрольного управления и Секретаря национальной безопасности), чтобы гарантировать -

"(A) использование соответствующих политик информационной безопасности, процедур и технологий, чтобы улучшить информационную безопасность и избежать ненужного и дорогостоящего дублирования усилий; и

"(B) что такие стандарты и руководства дополняют стандарты и руководства, используемые для защиты систем национальной безопасности и информации, содержавшейся в таких системах;

"(2) предоставлять обществу возможность прокомментировать предложенные стандарты и руководства;

"(3) представлять Министру торговли для обнародования в соответствии с разделом 11331 из заголовка 40, кодекса Соединенных Штатов -

"(A) стандарты, как требуется в подразделе (b) (1) (A), не позже чем через 12 месяцев после даты вступления в силу этого раздела; и

"(B) минимальные требования информационной безопасности для каждой категории, как требуется в подразделе (b) (1) (C), не позже чем через 36 месяцев после даты вступления в силу

этого раздела;

"(4) выпускать руководства, как требуется в подразделе (b) (1) (B), не позже чем через 18 месяцев после даты вступления в силу этого раздела;

"(5) до максимальной реальной степени гарантировать, что такие стандарты и руководства действительно не требуют использования или приобретения конкретных продуктов, включая любые конкретные аппаратные средства или программное обеспечение;

"(6) до максимальной реальной степени гарантировать, что такие стандарты и руководства предусматривают достаточную гибкость, чтобы разрешить альтернативным решениям обеспечить эквивалентные уровни защиты для идентифицированных рисков информационной безопасности; и

"(7) до максимальной реальной степени использовать гибкие, требующие реализации стандарты и руководства, которые позволяют использовать стандартные коммерчески разработанные продукты информационной безопасности.

"(d) ФУНКЦИИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. - Институт должен -

"(1) представлять стандарты, разработанные в соответствии с подразделом (a), наряду с рекомендациями относительно степени, до которой они следует быть сделаны обязательными и предписанными, Министру торговли для обнародования в соответствии с разделом 11331 из заголовка 40, кодекса Соединенных Штатов;

"(2) предоставлять техническую помощь агентствам, по запросу, относительно -

"(A) согласия со стандартами и руководствами, разрабатываемыми в подразделе (a);

"(B) обнаружения и обработки инцидентов информационной безопасности; и

"(C) политик, процедуры и методов информационной безопасности;

"(3) проводить исследования, при необходимости, чтобы определить характер и масштабы уязвимостей информационной безопасности и технологий для того, чтобы обеспечить рентабельную информационную безопасность;

"(4) разрабатывать и периодически пересматривать индикаторы выполнимости и меры для политик и методов информационной безопасности агентства;

"(5) оценивать политики и методы информационной безопасности частного сектора и коммерчески доступные информационные технологии, чтобы оценить их возможное применение агентствами для усиления информационной безопасности;

"(6) помогать частному сектору, по запросу, в использовании и применении результатов работ в соответствии с этим разделом;

"(7) оценивать политики и методы безопасности, разработанные для систем национальной безопасности, чтобы оценить их возможное применение агентствами для усиления информационной безопасности;

"(8) периодически оценивать эффективность стандартов и руководств, разработанных в соответствии с этим разделом, и осуществлять их пересмотр при необходимости;

"(9) запрашивать и принимать во внимание рекомендации Консультативного совета по Информационной безопасности и Приватности, установленного разделом 21, относительно стандартов и руководств, разработанных в подразделе (a), и представлять такие рекомендации Министру торговли вместе с представлением Министру этих стандартов; и

"(10) готовить ежегодный публичный отчет относительно работ предпринятых в предыдущем году и планируемых в наступающем году по выполнению обязанностей в соответствии с этим разделом.

"(e) ОПРЕДЕЛЕНИЯ. - использующиеся в этом разделе -

"(1) у термина 'агентство' есть то же самое значение как предусмотрено в разделе 3502 (1) из заголовка 44, кодекса Соединенных Штатов;

"(2) у термина 'информационная безопасность' есть то же самое значение как предусмотрено в разделе 3542 (b) (1) из этого заголовка;

"(3) у термина 'информационная система' есть то же самое значение как предусмотрено в разделе 3502 (8) из этого заголовка;

"(4) у термина 'информационная технология' есть то же самое значение как предусмотрено в разделе 11101 из заголовка 40, кодекса Соединенных Штатов; и

"(5) у термина 'система национальной безопасности' есть то же самое значение как предусмотрено в разделе 3542 (b) (2) из заголовка 44, кодекса Соединенных Штатов.

"(f) САНКЦИОНИРОВАНИЕ АССИГНОВАНИЙ. – санкционировано предоставить Министру торговли 20 000 000$ в течение каждого из бюджетных лет 2003, 2004, 2005, 2006 и 2007, чтобы дать возможность Национальному институту стандартов и технологий выполнить положения этого раздела".

СЕКЦИЯ 304. КОНСУЛЬТАТИВНЫЙ СОВЕТ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПРИВАТНОСТИ.

Раздел 21 из закона о Национальном институте стандартов и технологий (15 U.S.C. 278g-4), исправлен-

(1) в подразделе (a), исключено "Консультативный совет по безопасности и приватности компьютерных систем" и вставлено "Консультативный совет по информационной безопасности и приватности";

(2) в подразделе (a) (1), исключено "компьютер или телекоммуникации" и вставлено "информационная технология";

(3) в подразделе (a) (2) -

(A) исключено "компьютер или телекоммуникационная технология" и вставлено "информационная технология"; и

(B) исключено "компьютерное или телекоммуникационное оборудование" и вставлено "информационная технология";

(4) в подразделе (a) (3) -

(A) исключено "компьютерные системы" и вставлено "информационная система"; и

(B) исключено "безопасность компьютерных систем" и вставлено "информационная безопасность";

(5) в подразделе (b) (1), исключено "безопасность компьютерных систем" и вставлено "информационная безопасность";

(6) в подразделе (b) исключен параграф (2) и вставлен следующий:

"(2), чтобы советовать Институту, Министру торговли и Директору Министерства управления и бюджета по проблемам информационной безопасности и приватности, имеющим отношение к информационным системам Федерального правительства, включая через пересмотр предложенных стандартов и руководств, разрабатываемых в соответствии с разделом 20; и";

(7) в подразделе (b) (3), вставлено "ежегодно" после "отчета";

(8) вставлено после подраздела (e) следующий новый подраздел:

"(f) Совет должен проводить встречи на такой территории и в такое время и месте как определено большинством Совета.";

(9) переименованы подразделы (f) и (g) как подразделы (g) и (h), соответственно; и

(10) исключен подраздел (h), как переименованный параграфом (9), и вставлено следующее:

"(h) для использования в этом разделе, терминам 'информационная система' и 'информационная технология' даны значения в разделе 20.".

СЕКЦИЯ 305. ТЕХНИЧЕСКИЕ И СООТВЕТСТВУЮЩИЕ ПОПРАВКИ.

(a) ЗАКОН ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. - раздел 11332 из заголовка 40, кодекс Соединенных Штатов, и элемент, касающийся того раздела в таблице разделов для главы 113 такого заголовка, аннулированы.

(b) ЗАКОН САНКЦИОНИРОВАНИЯ НАЦИОНАЛЬНОЙ ОБОРОНЫ ФЛОЙД Д. СПЕНСЕРА НА 2001 БЮДЖЕТНЫЙ ГОД. - Закон о санкционировании национальной обороны Флойда Д. Спенсера на 2001 бюджетный год (Общественный закон 106-398) исправлен, исключением раздела 1062 (44 U.S.C. 3531 примечание).

(c) ЗАКОН О СОКРАЩЕНИИ ДОКУМЕНТОВ. - (1) Раздел 3504 (g) заголовка 44, кодекса Соединенных Штатов, исправлен -

(A) добавлением "и" в конце абзаца (1);

(B) в параграф (2) -

(i) исключены "разделы 11331 и 11332 (b) и (c) из заголовка 40" и вставлено "раздел 11331 из заголовка 40 и II подраздел этого раздела"; и

(ii) исключено"; и" и вставлен интервал; и

(C) исключен абзац (3).

(2) Раздел 3505 из такого заголовка исправлен добавлением в конце -

"(c) РЕЕСТР ГЛАВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ. - (1) руководитель каждого агентства должен разработать и сопровождать реестр главных информационных систем (включая главные системы национальной безопасности) управляемых или контролируемых таким агентством.

"(2) идентификация информационных систем в реестрах в этом подразделе должна включать идентификацию интерфейсов между каждой такой системой и всеми другими системами или сетями, включая те, которыми не управляет или не контролирует агентство.

"(3) Такие реестры должны быть -

"(A) обновлены, по крайней мере, ежегодно;

"(B) являться доступными для Генерального контролера; и

"(C) использоваться для поддержки управления информационными ресурсами, включая -

"(i) подготовку и поддержку реестров информационных ресурсов в разделе 3506 (b) (4);

"(ii) планирование, составление бюджета, приобретение и управление информационными технологиями в разделе 3506 (h), подзаголовок III заголовка 40, и соответствующих законов и руководств;

"(iii) мониторинг, тестирование и оценку мер информационной безопасности в подразделе II;

"(iv) подготовку указателя главных информационных систем, требуемого в разделе 552 (g) заголовка 5, кодекса Соединенных Штатов; и

"(v) подготовку реестра информационных систем, требуемых для управления записями в соответствии с разделами 21, 29, 31, и 33.

"(4) Директор должен выпустить руководство для и наблюдать за реализацией требований этого подраздела.".

(3) Раздел 3506 (g) такого заголовка исправлен -

(A) добавлено "и" в конце параграфа (1);

(B) в абзаце (2) -

(i) исключено "раздел 11332 из заголовка 40" и вставлено " подраздел II этого раздела"; и

(ii) исключено"; и" и вставлен интервал; и

(C) исключен параграф (3).

Секция 3502. Определения

(1) термин "агентство" означает любой исполнительный департамент, военный департамент, Правительственную корпорацию, Управляемую Правительством корпорацию или другое образование в исполнительной власти Правительства (включая исполнительное управление Президента) или любой независимый контролирующий орган, но не включает -

(A) Управление государственной ответственности;

(B) Федеральную избирательную комиссию;

(C) Правительства Округа Колумбия и территорий и владений Соединенных Штатов, и их различных подразделений; или

(D) Управляемые правительственным подрядчиком организации, включая лаборатории, участвующие в работах по исследованиям и производству для национальной обороны;

(2) термин " накладные расходы" означает время, усилие или финансовые ресурсы, израсходованные людьми по созданию,

сопровождению или предоставлению информации или для Федерального агентства, включая ресурсы, израсходованные для -

(A) рассмотрения инструкций;

(B) получению, установке и использованию технологий и систем;

(C) корректировке существующих способов выполнения любых ранее применяемых инструкций и требований;

(D) поиска источников данных;

(E) комплектования и пересмотра массивов информации;

и

(F) предоставления или иного раскрытия информации;

(3) термин "сбор информации" -

(A) означает получение, порождение для получения, обращение или требование по раскрытию третьим сторонам или обществу, фактов или суждений от или для агентства, независимо от формы или формата, вызванное любым -

(i) ответами на идентичные вопросы обращенные к, или идентичные требования создания отчетов или ведения записей, полученные от десять или больше человек, кроме агентств, средств или сотрудников Соединенных Штатов; или

(ii) ответами на вопросы обращенные к агентствам, средствам или сотрудникам Соединенных Штатов, которые должны использоваться для общих статистических целей; и

(B) не включает сбор информации, описанной под разделом 3518 (c) (1);

(4) термин "Директор" означает Директора Министерства управления и бюджета;

(5) термин "независимый контролирующий орган" означает Совет управляющих Федеральной резервной системы, Комиссия по торговле товарными фьючерсами, Комиссия по безопасности потребительских товаров, Федеральная комиссия по связи, Федеральная корпорация по страхованию депозитов, Федеральная энергетическая комиссия, Федеральное агентство по финансированию жилья, Федеральная морская комиссия, Федеральная торговая комиссия, Комиссия межгосударственной торговли, Комиссия по рассмотрению безопасности и здоровья в горной добыче, Национальное управление по занятости населения, Комиссия по ядерному урегулированию, Комиссия по рассмотрению охраны труда и медицины, Почтовая регулирующая Комиссия, Комиссия по ценным бумагам и биржам, и любое другое подобное агентство, определяемое уставом как федеральный независимый контролирующий орган или комиссия;

(6) термин "ресурсы информации" означает информацию и связанные ресурсы, такие как персонал, оборудование, фонды и информационные технологии;

(7) термин "управление ресурсами информации" означает процесс управления ресурсами информации для выполнения задач агентства и улучшения деятельности агентства, включая через сокращение трудностей сбора информации об обществе;

(8) термин "информационная система" означает отдельный набор ресурсов информации, организованных для сбора, обработки, поддержки, использования, совместного использования, распространения или размещения информации;

(9) термин "информационная технология" соответствует термину в разделе 11101 из заголовка 40, но не включает системы национальной безопасности, как определено в разделе 11103 из заголовка 40;

(10) термин "лицо" означает человека, партнерство, ассоциацию, корпорацию, коммерческий трест или юридического представителя, организованную группу людей, правительство Штата, территориальный, племенной или местный орган власти или его отделение, или политическое подразделение правительства Штата, территориального, племенного или местного органа власти или отделение политического подразделения;

(11) термин "практическая полезность" означает возможность агентства использовать информацию, особенно возможность обработать такую информацию своевременным и полезным способом;

(12) термин "общественная информация" означает любую информацию, независимо от формы или формата, которую агентство раскрывает, распространяет или делает доступной общественности;

(13) термин "требование ведения записей" означает требование, наложенное агентством или для агентства на людей по сопровождению определенных документов, включая требование к -

(A) сохранению таких документы;

(B) уведомлению третьих сторон, Федерального правительства или общества о существовании таких документов;

(C) раскрытию таких документов третьим сторонам, Федеральному правительству или обществу; или

(D) отчетности третьим сторонам, Федеральному правительству или обществу относительно таких документов; и

(14) термин "штраф" включает наложение агентством или судом взыскания или другого наказания; решение о денежном возмещении ущерба или эквивалентной компенсации; или аннулирование, приостановка, сокращение или отказ в лицензии, полномочии, праве, гранте или льготе.