ЦИРКУЛЯР № A-130
Пересмотренный
Переходящий Меморандум № 4
МЕМОРАНДУМ ДЛЯ РУКОВОДИТЕЛЕЙ ИСПОЛНИТЕЛЬНЫХ ДЕПАРТАМЕНТОВ И АГЕНТСТВ

Предмет: управление ресурсами Федеральной информации

1. Назначение: Этот Циркуляр устанавливает политику для управления ресурсами Федеральной информации. OMB содержит процедурные и аналитические руководящие положения для того, чтобы реализовать конкретные аспекты этих политик в приложениях.

2. Отмены: Этот Циркуляр отменяет Меморандумы OMB M-96-20, "Реализация Парламентской реформы управления информационными технологиями 1996;" M-97-02, "Консолидация инвестиций в информационные системы;" M-97-09, "Межведомственная поддержка для информационных технологий;" M-97-15, " Политика локальных телекоммуникационных сервисов;" M-97-16, "Архитектуры информационных технологии".

3. Полномочия: OMB выпускает этот Циркуляр в соответствии с Законом о сокращении документов (PRA) 1980, уточненным Законом о сокращении документов 1995 (44 U.S.C. Chapter 35); Законом Клингера-Коэна (также известным как "Парламентская реформа управления информационными технологиями 1996") (Pub. L. 104-106, Division E); Законом о неприкосновенности частной жизни, с уточнениями (5 U.S.C. 552a); Законом о финансовых директорах (31 U.S.C. 3512 et seq.) ; Законом о федеральный собственности и административных службах, с уточнениями (40 U.S.C. 487); Законом об информационной безопасности 1987 (Pub. L. 100-235); Законом о бюджете и бухгалтерском учете, с уточнениями (31 Глава 11 U.S.C.); Законом о Правительственной деятельности и Результатах, 1993 (GPRA); Законом о политике министерства федерального приобретения (41 Глава 7 U.S.C.); Правительственным законом о сокращении документов, 1998 (Pub. L. 105-277, Title XVII), Правительственным распоряжением № 12046 от 27 марта 1978; Правительственным распоряжением № 12472 от 3 апреля 1984; и Правительственным распоряжением № 13011 от 17 июля 1996.

4. Применимость и Область:

a. Политики в этом Циркуляре применяются к информационной деятельности всех агентств исполнительной власти Федерального правительства.
b. Информация, классифицированная как предназначенная для национальной безопасности, должна обрабатываться в соответствии с соответствующими директивами национальной безопасности. Работы в отношении национальной безопасности по подготовленности к чрезвычайным ситуациям должны быть проведены в соответствии с Правительственным распоряжением № 12472.

5. Фон: Закон Клингера-Коэна добавляет политики управления информационными ресурсами, содержавшиеся в PRA, устанавливая комплексный подход для исполнительных агентств, чтобы улучшить приобретение и управление их информационными ресурсами:

1. фокусирование планирования информационных ресурсов на поддержание их стратегического предназначения;
2. реализация процесса контроля основного планирования и инвестиций, связанного с формированием и выполнением бюджета; и
3. пересмотр и реструктурирование способов выполнения работ до осуществления вложений в информационные системы.

PRA устанавливает широкое предоставление полномочий для агентств по выполнению их работ управления информационными ресурсами в эффективном, рациональном и экономичном способе. Чтобы помочь агентствам в комплексном подходе к управлению информационными ресурсами, PRA требует, чтобы Директор OMB разработал и реализовал универсальные и непротиворечивые политики управления информационными ресурсами; наблюдал за разработкой и способствовал использованию принципов, стандартов и руководящих положений по управлению информацией; оценивал методы управления информационными ресурсами агентств, чтобы определить их соответствие и действенность; и определял согласие таких методов с политиками, принципами, стандартами и руководящими положениями, провозглашенными Директором.

6. Определения:

a. Термин "агентство" означает любой исполнительный департамент, военный департамент, правительственную корпорацию, корпорацию контролируемую правительством или другое учреждение в исполнительной власти Федерального правительства или любой независимый контролирующий орган. В пределах исполнительного управления Президента термин включает только OMB и Администрацию.

b. Термин "аудиовизуальная продукция" означает объединенное представление, разработанное согласно плану или сценарию, содержащее визуальное изображение, звук или оба и используемое для передачи информации.

c. Термин " процесс капитального планирования и управления инвестициями " означает процесс управления постоянной идентификацией, выбором, контролем и оценкой инвестиций в информационные ресурсы. Процесс связывает формирование и выполнение бюджета, и фокусируется на предназначении агентства и достижении конкретных программных результатов.

d. Термин "Совет Директоров по информации" (CIO Совет) означает Совет, установленный в Разделе 3 из Правительственного распоряжения 13011.

e. Термин "распространение" означает инициированное правительством предоставление информации обществу. Не считается распространением в рамках назначения этого Циркуляра распределение, ограниченное правительственными сотрудниками или подрядчиками или получателями агентства, использование или совместное использование правительственной информации внутри или между агентствами, и реакции на запросы на документы агентства, связанные с Законом о свободе информации (5 U.S.C. 552) или Законом о неприкосновенности частной жизни.

f. Термин "исполнительное агентство" имеет значение, определенное в разделе 4 (1) из Закона о Министерстве федеральной политики приобретения (41 U.S.C. 403 (1)).

g. Термин "полные стоимости," когда применяется к расходам, понесенным в деятельности организации, обслуживающей обработку информации (IPSO), состоит из всех прямых, косвенных, общих и административных расходов, понесенных в деятельности IPSO. Эта стоимость включает, но не ограничена, персонал, оборудование, программное обеспечение, принадлежности, контрактные сервисы от поставщиков частного сектора, использование помещений, внутриагентские сервисы, межведомственных сервисы от других Федеральных агентств, другие услуги, которые предоставлены правительствами штатов и местными органами власти, и организациями Судебной и Законодательной власти.

h. Термин "правительственная информация" означает информацию, создаваемую, собираемую, обрабатываемую, распространяемую или ликвидируемую для или из Федерального правительства.

i. Термин "правительственная публикация" означает информацию, которая опубликована как отдельный документ за правительственный счет или как требуется законом. (44 U.S.C. 1901)

j. Термин "информация" означает любую передачу или представление знаний, таких как факты, данные или мнения на любом носителе или в любой форме, включая текстовую, числовую, графическую, картографическую, описательную или аудиовизуальную формы.

k. Термин " продукт распространения информации " означает любую книгу, газету, карту, машиночитаемый материал, аудиовизуальную продукцию или другой документальный материал, независимо от физической формы или характеристик, распространяемый агентством среди общества.

l. Термин " жизненный цикл информации " означает стадии, через которые информация проходит, обычно характеризуемые как создание или сбор, обработка, распространение, использование, хранение и ликвидация.

m. Термин "управление информацией" означает планирование, составление бюджета, манипулирование и контроль информации всюду по её жизненному циклу.

n. Термин "информационные ресурсы" включает правительственную информацию и информационные технологии.

o. Термин "организация, обслуживающая обработку информации" (IPSO) означает дискретный набор персонала, информационных технологий и вспомогательного оборудования с основной функцией предоставления услуг более чем одному агентству на возмездной основе.

p. Термин " управление информационными ресурсами" означает процесс управления информационными ресурсами выполняемый в соответствии с предназначением агентства. Термин охватывает и непосредственно информацию и связанные ресурсы, такие как персонал, оборудование, фонды и информационные технологии.

q. Термин "информационная система" означает дискретный набор информационных ресурсов, организованных для сбора, обработки, поддержки, передачи и распространения информации, в соответствии с определенными автоматизированными или ручными процедурами.

r. Термин "жизненный цикл информационной системы" означает фазы, через которые информационная система проходит, обычно характеризуемые как инициирование, разработка, эксплуатация и ликвидация.

s. Термин "информационная технология" означает любое оборудование или объединенную систему или подсистему оборудования, которое используется в автоматизированном приобретении, хранении, манипулировании, управлении, перемещении, контроле, показе, переключении, обмене, передаче или приеме данных или информации исполнительным агентством. Для назначения предыдущего предложения, оборудование используется исполнительным агентством, если оборудование используется исполнительным агентством непосредственно или используется подрядчиком в соответствии с контрактом с исполнительным агентством который: (i) требует использования такого оборудования; или (ii) требует использования, до существенной степени, такого оборудования в реализации сервиса или оснащении продукта. Термин информационная технология включает компьютеры, вспомогательное оборудование, программное обеспечение, встроенное микропрограммное обеспечение и подобные процедуры, сервисы (включая службу поддержки) и связанные ресурсы. Термин "информационная технология" не включает любое оборудование, которое получено федеральным подрядчиком помимо федерального контракта. Термин "информационная технология" не включает системы национальной безопасности, как определено в законе Клингера-Коэна 1996 (40 U.S.C. 1452).

t. Термин "Совет по ресурсам информационных технологий" (Совет по ресурсам) означает совет, установленный Разделом 5 из Правительственного распоряжения 13011.

u. Термин "главная информационная система" означает информационную систему, которая требует специального внимания управления из-за её важности для предназначения агентства; высоких затрат на её разработку, эксплуатацию или поддержку; или её существенной роли в администрировании программ, финансов, собственности или других ресурсов агентства.

v. Термин "система национальной безопасности" означает любые телекоммуникации или информационную систему, которой управляет Правительство Соединенных Штатов, функция, эксплуатация или использование которой (1) включают разведывательную деятельность; (2) включают криптологические работы, связанные с национальной безопасностью; (3) включают руководство и управление вооруженными силами; (4) включают оборудование, которое является неотъемлемой частью оружия или системы оружия; или (5) являются критическими по отношению к прямому выполнению военных или задач разведки, но исключая любую систему, которая должна использоваться для стандартных административных и бизнес-приложений (включая

платежи, финансы, логистику и приложения управления персоналом). Политики и процедуры, установленные в этом Циркуляре, применяются к системам национальной безопасности в способе, непротиворечивом с применением и связанными ограничениями относительно таких систем, изложенными в Разделе 5141 из закона Клингера-Коэна (Pub. L. 104-106, 40 U.S.C. 1451). Применение закона Клингера-Коэна к системам национальной безопасности должна включать требования подготовки бюджетных документов, установленные в Циркуляр OMB A-11. Результирующий бюджетный документ может быть классифицирован в соответствии с положениями Правительственного распоряжения 12958.

w. Термин "записи" означает все книги, бумаги, карты, фотографии, машиночитаемые материалы или другие документальные материалы, независимо от физической формы или характеристик, сделанные или полученные агентством Правительства Соединенных Штатов в соответствии с Федеральным законом или в соответствии с общей деятельностью и сохраненные или подготовленные для сохранения этим агентством или его законным преемником как свидетельство структуры, функций, политик, решений, процедур, деятельности или других работ правительства или из-за информационного значения данных в них. Не включает библиотечные и музейные материалы, сделанные или полученные и сохраненные исключительно для ссылочного или выставочного назначения, дополнительные копий документов, сохраненные только для удобства ссылки, и запасы публикаций и обработанных документов. (44 U.S.C. 3301)

x. Термин " управление записями " означает планирование, контроль, направление, организацию, обучение, продвижение и другие организаторские работы, примененные к созданию записей, поддержке и использованию записей, и ликвидация записей, для достижения адекватного и надлежащего документирования политик и действий Федерального правительства и эффективного и экономичного управления деятельностью агентства. (44 U.S.C. 2901 (2))

y. Термин "получатель сервиса" означает организационную единицу агентства, программную сущность или ответственную учетную запись, которая получает сервисы обработки информации от организации, обслуживающей обработку информации (IPSO). Получатель сервиса, может быть как внутренним, так и внешним по отношению к организации, ответственной за предоставление услуг информационных ресурсов, но обычно не подотчетным менеджеру или директору IPSO или некоторому непосредственному руководителю.

7. Основные соображения и предположения:

a. Федеральное правительство - крупнейший самостоятельный производитель, собиратель, потребитель и распределитель информации в Соединенных Штатах. Учитывая значимость информационных действий правительства и влияния этих действий на общую кооперацию, управление ресурсами Федеральной информации - проблема постоянной значимости для всех Федеральных агентств, правительств штатов и местных органов власти и общества.

b. Правительственная информация - ценные национальные ресурсы. Она предоставляет обществу сведения относительно правительства, общества и экономики - прошлые, настоящие и будущие. Это - средство гарантировать подконтрольность правительства, управлять деятельностью правительства, поддерживать здоровую производительность экономики и является самостоятельно товаром на рынке.

c. Свободный поток информации между правительством и обществом важен для демократического общества. Также важно, что правительство минимизирует федеральное

бремя документов для общества, минимизирует стоимость его информационных действий и максимизирует полноценность правительственной информации.

d. Чтобы минимизировать стоимость и максимизировать полноценность правительственной информации, ожидаемые общественные и частные льготы, полученные из правительственной информации, должны превысить общественную и частную стоимость информации, понимая, что льготы, которые будут получены из правительственной информации, могут не всегда быть измеримыми.

e. Нация может извлечь выгоду из правительственной информации, распространяемой и Федеральными агентствами и разнообразными не федеральными участниками, включая агентства правительств штатов и местных органов власти, образовательные и другие некоммерческие учреждения и коммерческие организации.

f. Поскольку общее раскрытие правительственной информации важно для деятельности демократии, управление ресурсами Федеральной информации должно защищать право общества на доступ к правительственной информации.

g. Право человека на приватность должно быть защищено в информационных действиях Федерального правительства, включающих персональные данные.

h. Систематизированное внимание к управлению правительственными записями - важная составляющая осмысленного общественного управления ресурсами, которое гарантирует общественную подконтрольность. Совместно с сохранением документов, это защищает исторические документы правительства и охраняет законные и финансовые права правительства и общества.

i. Стратегическое планирование улучшает деятельность государственных программ. Стратегический план агентства формирует модернизацию процессов работы и является руководством по разработке и поддержке Архитектуры предприятия и основного планирования и процесса управления инвестициями. Этот подход управления способствует соответствующему приложению ресурсов Федеральной информации.

j. Поскольку правительства штатов и местные органы власти - важные производители правительственной информации для многих областей, таких как здоровье, социальное обеспечение, рабочая сила, перевозки и образование, Федеральное правительство должно сотрудничать с этими правительствами в управлении информационными ресурсами.

k. Открытый и эффективный обмен научно-технической правительственной информацией согласно применимым мерам обеспечения национальной безопасности и правомочиям других собственников, способствует превосходству в научных исследованиях и эффективном использовании федеральных научно-исследовательских фондов.

l. Информационные технологии – не самоцель. Это – один из набора ресурсов, которые могут улучшить эффективность и действенность федеральной программы поставок.

m. Политики и действия по управлению информационными ресурсами Федерального правительства могут влиять на и быть подверженными влиянию со стороны информационных политик и действий других наций.

n. У пользователей ресурсов Федеральной информации должны быть квалификация, знания и обучение, чтобы управлять информационными ресурсами, давая возможность Федеральному правительству эффективно служить обществу через автоматизированные средства.

o. Применение актуальных информационных технологий предоставляет возможности способствовать коренным изменениям в структурах агентства, рабочих процессах и способах взаимодействия с обществом, которые улучшают эффективность и действенность Федеральных агентств.

p. Доступность правительственной информации на разнообразных носителях информации, включая электронные форматы, предоставляет агентствам и обществу большую гибкость в использовании информации.

q. Федеральные руководители с обязанностями по формированию программ должны осознать важность управления информационными ресурсами в достижении результатов деятельности.

r. Совет Директоров по информации и Совет по ресурсам информационных технологий должны помогать в разработке и использовании межведомственных и межоперационных совместно используемых информационных ресурсов для поддержки выполнения правительственной деятельности.

8. Политика:

a. Политика управления информацией

1. Как агентства проводят планирование управления информацией?

Агентства должны планировать управление информацией в интегрированном способе всюду по ее жизненному циклу. Агентства должны:

……..

2. Каковы руководящие принципы по сбору информации?

Агентства должны собирать или создать только ту информацию, которая необходима для надлежащего выполнения функций агентства и у которой есть практическая полезность.

3. Каковы руководящие принципы для сбора электронной информации?

Исполнительные агентства с соответствии с Разделами 1703 и 1705 Правительственного акта об Устранении Документов (GPEA), P. L. 105-277, Заголовок XVII, обязаны обеспечить к 21 октября 2003, (1) вариант электронной поддержки, представления или разглашения информации, когда это практично вместо бумаги; и (2) использование и одобрение электронных подписей, когда это практично. Агентства будут следовать за положениями Меморандума OMB M. 00 10, "Процедуры и руководство по реализации правительственного акта о сокращении документов."

4. Как агентства должны реализовать управление документами?

……..

5. Как агентство должно предоставлять информацию обществу?

   Агентства несут ответственность за предоставление обществу информации, соответствующей их предназначению. Агентства реализуют эту ответственность:

   ……

6. Какова Система управления распространением информации?

   ……

7. Как агентства должны избегать нарушений свободы конкуренции?

   ……

8. Как агентства должны выполнять электронное распространение информации?

   ……

9. Каким мерам защиты агентства должны следовать?

   Агентства должны:

   (a) Гарантировать, что информация защищена соразмерная с риском и величиной вреда, который следовал бы из потери, неправильного употребления или несанкционированного доступа к или модификации такой информации;

   (b) Ограничивать набор информации, которая идентифицирует людей, до такого, который по закону санкционирован и необходим для надлежащего выполнения функций агентства;

   (c) Ограничивать обмен информацией, которая идентифицирует людей или содержит конфиденциальную информацию до такого, который санкционирован по закону, и налагать соответствующие условия на использование там, где существуют действующие обязательства гарантировать конфиденциальность информации;

   (d) Предоставлять людям, по запросу, доступ к записям о них, поддерживаемых в системах в соответствии с Законом о неприкосновенности частной жизни, и разрешать им исправлять такие записи, если они противоречивы с положениями Закона о неприкосновенности частной жизни.

b. Как Агентства должны управлять информационными системами и информационными технологиями?

   (1) Как агентства должны использовать основное планирование и процесс контроля инвестиций?

……

(2) Архитектура предприятия (EA)

Агентства должны задокументировать и представить OMB свою начальную EA. Агентства должны представлять обновления, когда существенные изменения в Архитектуре предприятия происходят.

(a) Что такое Архитектура предприятия?

EA - явное описание и документирование текущих и требуемых отношений между деятельностью, процессами управления и информационными технологиями. Она описывает "текущую архитектуру" и "целевую архитектуру", чтобы включить информацию о правилах, стандартах и жизненном цикле систем для оптимизации и сопровождения среды, которую агентство хочет создать и сопроводить, управляя его портфелем ИТ. EA должна также обеспечить стратегию, которая даст возможность агентству поддержать свое текущее состояние и также действовать как путеводитель для перехода к его целевой среде. Эти процессы перехода будут включать основное планирование агентства и процессы контроля инвестиций, процессы планирования EA агентства и методологию жизненного цикла систем агентства. EA определяет принципы и цели и концентрирует внимание на таких проблемах как продвижение функциональной совместимости, открытости систем, открытости доступа, согласия с GPEA, удовлетворение конечного пользователя и безопасность IT-систем. Агентство должно поддерживать EA полным составом информационных ресурсов агентства, включая персонал, оборудование и фонды, выделяемые на управление информационными ресурсами и информационными технологиями, в соответствующем уровне детализации. Агентства должны реализовать EA, непротиворечивую со следующими принципами:

(i) Разрабатывать информационные системы, которые облегчают функциональную совместимость, мобильность приложения и расширяемость электронных приложений через сети неоднородных аппаратных средств, программного обеспечения и телекоммуникационных платформ;

(ii) Удовлетворять потребности в информационных технологиях через экономически выгодное использование внутренних и внешних возможностей, прежде чем приобретать новые ресурсы информационных технологий; и

(iii) Устанавливать уровень безопасности для всех информационных систем, который соразмерен риску и величине вреда, следующего из потери, неправильного употребления, несанкционированного доступа к, или модификации хранящейся или передаваемой через эти системы информации.

(b) Как агентства создают и сопровождают EA?

Как часть усилия по EA, агентства должны использовать или создавать Основу Архитектуры предприятия. Основа должна документировать связи между потребностями предназначения, информационным контентом и возможностями информационных технологий. Основа должна быть также руководством к стратегическому и операционному IRM, планированию.

Как только основа установлена, агентство должно создать EA. При создании EA агентства должны идентифицировать и документировать:

(i) Бизнес-процессы - Агентства должны идентифицировать работу, выполняемую, чтобы поддержать его предназначение, перспективы и результирующие цели. Агентства должны также документировать источники изменений, такие как законодательство или новые технологии, которые будут инициировать изменения в EA.

(ii) Передача и обмен информацией - Агентства должны проанализировать информацию, используемую агентством в его бизнес-процессах, идентифицируя используемую информацию и передачу информации. Эти информационные потоки указывают, где информация необходима и как информацией делятся, чтобы поддержать функции предназначения.

(iii) Приложения - Агентства должны идентифицировать, определить и организовать работы, которые получают, манипулируют и управляют бизнес-информацией, чтобы поддержать процессы деятельности. EA также описывает логические зависимости и отношения между деловыми операциями.

(iv) Описания и взаимосвязь данных - Агентства должны идентифицировать, как данные созданы, сопровождены, получается доступ к ним и используются. На высоком уровне агентства должны определить данные и описать отношения среди элементов данных, используемых в информационных системах агентства.

(v) Технологическая инфраструктура - Агентства должны описать и идентифицировать функциональные характеристики, возможности и взаимосвязи аппаратных средств, программного обеспечения, и телекоммуникаций.

(c) Какова Модель технического справочника и Профиль стандартов?

EA должен также включать Модель технического справочника (TRM) и Профиль стандартов.

(i) TRM идентифицирует и описывает информационные услуги (такие как база данных, связь, интранет и т.д.) используемые всюду по агентству.

(ii) Профиль стандартов определяет набор стандартов ИТ, которые поддерживают сервисы, ясно сформулированные в TRM. Агентства, как ожидается, примут стандарты, необходимые, чтобы поддержать всю EA, которая должна быть определена по всему агентству.

(iii) Как часть Профиля стандартов, агентства должны создать Профиль стандартов обеспечения безопасности, который конкретен к сервисам безопасности, определенным в EA, и закрывает такие сервисы как идентификация, аутентификация и неотказуемость; создание и анализ журнала аудита; контроль доступа; управление криптографией; антивирусная защита; предотвращение мошенничества; обнаружение и смягчение; и предотвращение и обнаружение вторжений.

(3) Как Агентства гарантируют безопасность в информационных системах?

Агентства должны включить безопасность в архитектуру их информации и систем, чтобы гарантировать, что безопасность поддерживает деятельность агентства и что планы финансирования и управления безопасностью встроены в бюджеты жизненного цикла для информационных систем.

(a) Чтобы поддержать более эффективную реализацию агентством компьютерной безопасности агентства и программ защиты критической инфраструктуры, агентства должны реализовать следующее:

(i) Распределение по приоритетам ключевых систем (включая те, которые являются самыми критическими по отношению к деятельности агентства);
(ii) Применение политики OMB и, для приложений, не относящихся к национальной безопасности, руководств NIST, для достижения адекватной безопасности, соразмерной с уровнем риска и величиной вреда;

(b) Агентства должны сделать роль безопасности явной в инвестициях в информационные технологии и основных программах. Инвестиции в разработку новых или поддержание эксплуатации существующих информационных систем, как для общих систем поддержки так и для главных приложений должны:

(i) Демонстрировать, что меры безопасности для компонентов, приложений и систем непротиворечивы с, и являются неотъемлемой частью EA агентства;

(ii) Демонстрировать, что стоимость мер безопасности понята и явно включена в жизненный цикл планирования всей системы в способе, непротиворечивом с руководством OMB для основного планирования;

(iii) Включать план обеспечения безопасности, который выполняет Приложение III этого Циркуляра и который непротиворечив с руководством NIST по планировании обеспечения безопасности;

(iv) Демонстрировать, что конкретные используемые методы гарантируют, что риски и потенциальные потери поняты и непрерывно оцениваются, что сделаны шаги, чтобы поддерживать риск на допустимом уровне, и что процедуры на месте должны гарантировать, что меры обеспечения безопасности реализованы эффективно и остаются эффективными в течение долгого времени;

(v) Демонстрировать, что конкретные используемые методы гарантируют, что меры безопасности соразмерны с риском и величиной вреда, который может следовать из потери, неправильного употребления или несанкционированного доступа к или модификации системы непосредственно или информации, которой она управляет;

(vi) Идентифицировать дополнительные меры безопасности, которые необходимы, чтобы минимизировать риск к и возможные потери от тех систем, которые поддерживают или разрешают открытый доступ, других внешних доступных систем и тех систем, которые соединены с системами, над которыми должностные лица программы имеют небольшой или никакой контроль;

(vii) Развернуть эффективные меры безопасности и инструменты аутентификации, непротиворечивые с защитой приватности, такие как цифровая подпись, базирующаяся на открытых ключах, для тех систем, которые поддерживают или разрешают открытый доступ;

(viii) Гарантировать, что обработка персональных данных непротиворечива с соответствующими обще-правительственными и обще-агентскими политиками;

(ix) Описывать каждый случай, когда агентство решает использовать стандарты и руководство, которые являются более строгими чем провозглашенные NIST, чтобы гарантировать использование основанных на риске рентабельных мер безопасности для приложений безопасности, не относящихся к национальной безопасности;

(c) OMB будет рассматривать для нового или продолжающегося финансирования только те инвестиции в системы, которые удовлетворяют этим критериям. Новые инвестиции в информационные технологии должны демонстрировать, что существующие системы агентства также соответствуют этим критериям, чтобы иметь право на финансирование.

(4) Как Агентства должны получать информационные технологии?

Агентства должны:

(a) Получая информационную технологию использовать адекватную конкуренцию, разделение рисков между правительством и подрядчиком и максимизировать доход от инвестиций;

(b) Структурировать главные информационные системы в конструктивные сегменты с узкой областью и краткой продолжительностью. Это должно уменьшить риск, способствовать гибкости и функциональной совместимости, увеличению подконтрольности и лучшему соответствию потребности предназначения с современными технологиями и состоянием рынка;

(c) Получать массовое ПО из коммерческих источников, если эффективность издержек на разработку заказного программного обеспечения не является четкой и не была подтверждена через экспериментальные проекты или прототипы; и

(d) Гарантировать доступность полученных информационных технологий в соответствии с Законом о реабилитации 1973, с уточнениями (Закон 105-220, 29 U.S.C.794d Pub.).

9. Назначение обязанностей:

a. Все Федеральные агентства. Руководитель каждого агентства должен:

……..

b. Госдепартамент. Госсекретарь должен:

……

c. Министерство торговли. Министр торговли должен:

……..

d. Министерство обороны.

……

e. Управление служб общего назначения.

……

f. Офис Управления персоналом.

……

g. Национальное управление архивов и документации.

……..

h. Министерство управления и бюджета.

……

10. Надзор:

……

11. Вступление в силу: Этот Циркуляр вступает в силу с момента выпуска. Ничто в этом Циркуляре не должно рассматриваться как предоставление частных прав на действия для любого человека.

12. Запросы: Все вопросы или запросы должны адресоваться Управлению информационных и регулирующих дел, Министерства управления и бюджета, Вашингтон, округ Колумбия 20503. Телефонный: (202) 395-3785.

13. Дата Пересмотра заката: OMB пересмотрит этот Циркуляр через три года от даты выпуска, чтобы установить его эффективность.

Приложение III к Циркуляру OMB № A-130

Безопасность Федеральных автоматизированных информационных ресурсов

A. Требования.

1. Назначение

Это Приложение устанавливает минимальный набор мер безопасности, которые будут включены в федеральные программы безопасности автоматизированной информации; возлагает на Федеральные агентства обязанности по безопасности автоматизированной информации; и связывает программы агентства по безопасности автоматизированной информации и меры

агентств по управлению системами, установленные в соответствии с Циркуляром OMB № A-123. Приложение пересматривает процедуры, прежде содержавшиеся в Приложении III к Циркуляру OMB № A-130 (50 FR 52730; 24 декабря 1985), и включает требования Закона об информационной безопасности от 1987 (P.L. 100-235), и обязанности возложенные в применимых директивах национальной безопасности.

2. Определения

Термин:

a. "адекватная безопасность" означает безопасность, соразмерную с риском и величиной вреда, следующего из потери, неправильного употребления или несанкционированного доступа к или модификации информации. Это включает доверие к тому, что системы и приложения, используемые агентством, применяются эффективно и обеспечивают соответствующую конфиденциальность, целостность и доступность с помощью рентабельных организационных, управления персоналом, эксплуатационных и технических мер безопасности.

b. "приложение" означает использование информационных ресурсов (информации и информационных технологий) для удовлетворения конкретному набору требований пользователя.

c. " система общей поддержки" или "система" означают взаимосвязанный набор информационных ресурсов под некоторым прямым административным управлением, которые предоставляют общую функциональность. Система обычно включает аппаратные средства, программное обеспечение, информацию, данные, приложения, связь и людей. Система может быть, например, локальной сетью (LAN), включая интеллектуальные терминалы, которая поддерживает филиалы, обще-агентскую магистраль, систему коммуникаций, ведомственный центр обработки данных, включая его операционную систему и утилиты, тактическую радиосеть, или совместно используемую организацию, обслуживающую обработку информации (IPSO).

d. "главное приложение" означает приложение, которое требует особого внимания к безопасности вследствие риска и величина вреда, следующего из потери, неправильного употребления или несанкционированного доступа к или модификации информации в приложении. Примечание: Все федеральные приложения требуют некоторого уровня защиты. Однако некоторые приложения, из-за информации в них, требуют специального надзора руководства и должны быть рассмотрены как главные. Адекватная безопасность для других приложений должна быть обеспечена безопасностью систем, в которых они работают.

3. Программы безопасности автоматизированной информации. Агентства должны реализовывать и сопровождать программу, чтобы гарантировать, что адекватная безопасность обеспечена для всей информации агентства собираемой, обрабатываемой, передаваемой, хранимой или распространяемой в системах общей поддержки и главных приложениях.

Программа каждого агентства должна реализовывать политики, стандарты и процедуры, которые непротиворечивы с политиками, стандартами и процедурами всего правительства, выпущенными Министерством управления и бюджета, Министерством торговли, Администрацией служб общего назначения и Офисом управления персоналом (OPM). Отличающиеся или более строгие

требования для того, чтобы обеспечить безопасность информации национальной безопасности должны быть включены в программы агентства, как требуется соответствующими директивами национальной безопасности. Как минимум, программы агентства должны включать следующие меры безопасности в свои системы общей поддержки и главные приложения:

a. Меры безопасности для систем общей поддержки.

1) Возложение ответственности за безопасность. Возложите ответственность за безопасность в каждой системе на человека, хорошо осведомленного в информационной технологии, используемой в системе и в обеспечении безопасности для такой технологии.

2) План безопасности системы. План адекватной безопасности каждой системы общей поддержки является частью процесса планирования управления информационными ресурсами организации (IRM). План обеспечения безопасности должен быть непротиворечивым с руководством, выпущенным Национальным институтом стандартов и технологий (NIST). Независимые рекомендации и комментарии к плану обеспечения безопасности должны требоваться до реализации плана. В стратегический план IRM, требуемый законом о Сокращении Документов (44 Главы 35 U.S.C.) и Разделом 8 (b) этого циркуляра, должна быть включена сводка планов обеспечения безопасности. Планы обеспечения безопасности должны включать:

a) Правила системы. Установите ряд правил, касающихся поведения, использования, безопасности и допустимого уровня риска для системы. Правила должны быть основаны на потребностях различных пользователей системы. Безопасность, требуемая правилами, должна быть строгой ровно на столько, на сколько необходимо, чтобы обеспечить адекватную безопасность для информации в системе. Такие правила должны ясно очерчивать обязанности и ожидаемое поведение всех людей с доступом к системе. Они должны также включать соответствующие ограничения на соединения с другими системами и определять предоставление услуг и приоритеты восстановления. Наконец, они должны определять последствия поведения, не согласующегося с правилами.

b) Обучение. Гарантируйте, что все люди соответственно обучены тому, как выполнять их обязанности по безопасности прежде, чем предоставить им доступ к системе. Такое обучение должно гарантировать, что сотрудники являются сведущими в правилах системы, быть непротиворечивым с руководством, выпущенным NIST и OPM и информировать их о доступной помощи и технических продуктах и технологиях безопасности. Для продолжения доступа к системе должны требоваться поведение, непротиворечивое с правилами системы, и периодическая переподготовка.

c) Меры безопасности персонала. Контролируйте людей, которые имеют полномочия на обход существенных технических и эксплуатационных мер безопасности системы, соразмерно с риском и величиной ущерба, который они могут нанести. Такой контроль должен осуществляться до предоставления человеку полномочий по обходу мер безопасности и периодически после этого.

d) Способность реагирования на инциденты. Гарантируйте, что есть возможность обеспечить помощь пользователям, когда инцидент безопасности происходит в

системе и предоставить информацию относительно общих уязвимостей и угроз. Эта способность должна обеспечиваться общей информацией с другими организациями, координируемыми NIST, и должна помогать агентству в проведении соответствующего расследования, непротиворечивого с руководством Министерства юстиции.

e) Непрерывность поддержки. Установите и периодически тестируйте способность продолжать предоставление услуг в системе, основанную на потребностях и приоритетах участников системы.

f) Техническая безопасность. Гарантируйте, что в системе используются соответствующие рентабельные продукты и технологии безопасности.

g) Взаимосвязь систем. Получите письменные руководящие указания, основанные на принятии риска к системе до соединения с другими системами. Там где разрешается соединение, должны быть установлены меры безопасности, которые непротиворечивы с правилами системы и в соответствии с руководством от NIST.

3) Пересмотр мер безопасности. Пересматривайте меры безопасности в каждой системе, когда в системе делаются существенные модификации, но, по крайней мере, каждые три года. Область и частота пересмотра должны быть соразмерными с допустимым уровнем риска для системы. В зависимости от потенциального риска и величины вреда, который может произойти, рассмотрите идентификацию недостатков в соответствии с Циркуляром OMB № A-123, "Целевое управление и контроль" и законом о федеральных менеджерах финансовой целостности (FMFIA), если отсутствует присвоение ответственности за обеспечение безопасности, план обеспечения безопасности или санкционирование на обработку для системы.

4) Санкционирование на обработку. Гарантируйте, что имеется официальное санкционирование должностного лица администрации в письменной форме на использование каждой системы общей поддержки, основанное на реализации ее плана обеспечения безопасности прежде, чем начать или значительно изменить обработку в системе. Использование систем должно быть повторно санкционировано, по крайней мере, каждые три года.

b. Меры безопасности для Главных приложений.

1) Возложение ответственности за безопасность. Возложите ответственность за безопасность каждого главного приложения на официальное должностное лицо, хорошо осведомленное в сущности информации и процессе, поддерживаемом приложением, и в организационных, управления персоналом, эксплуатационных и технических мерах безопасности, используемых для их защиты. Это должностное лицо должно гарантировать, что в приложении используются соответствующие эффективные продукты и технологии безопасности, и быть доступным, когда инцидент безопасности происходит относительно приложения.

2) План безопасности приложений. План адекватной безопасности каждого главного приложения, принимающий во внимание безопасность всех систем, в которых будет работать приложение. План должен быть непротиворечивым с руководством,

выпущенным NIST. До реализации плана должны требоваться рекомендации и комментарии к плану от должностного лица, ответственного за безопасность в основной системе, в которой приложение будет работать. В стратегический план IRM, требуемый законом о сокращении документов, должна быть включена сводка планов обеспечения безопасности. Планы безопасности приложений должны включать:

a) Правила приложения. Установите набор правил, касающихся использования и режимов приложения. Правила должны быть строгими насколько, насколько необходимо, чтобы обеспечить адекватную безопасность для приложения и информации в нем. Такие правила должны ясно очерчивать обязанности и ожидаемое поведение всех людей с доступом к приложению. Кроме того, правила должны определять последствия поведения, не согласующегося с правилами.

b) Специализированное обучение. Прежде чем предоставить доступ людей к приложению гарантируйте, что все люди получили специализированное обучение, сосредоточенное на их обязанностях и правилах приложения. Это может быть в дополнение к обучению, требующемуся для доступа к системе. Такое обучение может варьироваться от информирования во время допуска (например, для публичных пользователей, использующих приложение для информационного поиска), до формального обучению (например, для сотрудника, который работает с рискованным приложением).

c) Безопасность персонала. Включите меры безопасности, такие как разделение ответственности, наименьшее количество полномочия и индивидуальная подконтрольность в приложение и правила приложения как соответствующе. В случаях, когда такие меры безопасности не могут соответственно защитить приложение или информацию в нем, контролируйте людей, соразмерно с риском и величиной ущерба, который они могут нанести. Такой контроль должен осуществляться до того, как люди допускаются к приложению и периодически после того.

d) Планирование на случай непредвиденных ситуаций. Установите и периодически тестируйте способность агентства выполнить функцию, поддержанную приложением, в случае отказа его автоматизированной поддержки.

e) Технические меры безопасности. Гарантируйте, что соответствующие меры безопасности определены, разработаны, протестированы и приняты в приложении в соответствии с соответствующим руководством, выпущенным NIST.

f) Совместное использование информации. Гарантируйте, что информация, предоставляемая от приложения, защищена соответственно, сопоставимо с защитой обеспечиваемой тогда, когда информация находится в пределах приложения.

g) Меры обеспечения открытого доступа. Когда приложение агентства поддерживает или разрешает открытый доступ, дополнительные меры безопасности должны быть добавлены, чтобы защитить целостность

приложения и доверительность, которую общество имеет в отношении приложения. Такие меры безопасности должны включать разделение информации, делаемой непосредственно доступной обществу, от официальных записей агентства.

3) Пересмотр мер безопасности приложения. Выполняйте независимый пересмотр или аудит мер безопасности в каждом приложении, по крайней мере, каждые три года. Рассматривайте идентификацию недостатков в соответствии с Циркуляром OMB № A-123, "Целевое управление и контроль" и Законом о федеральных менеджерах финансовой целостности (FMFIA), если отсутствует присвоение ответственности за обеспечение безопасности, план обеспечения безопасности или санкционирование на обработку для системы.

4) Санкционирование на обработку. Гарантируйте, что имеется официальное санкционирование должностного лица администрации в письменной форме на использование приложения, подтверждающее, что реализованный план обеспечения его безопасности адекватно обеспечивает безопасность приложения. Результаты нового пересмотра или аудит мер обеспечения должны быть фактором в официальном санкционировании. Приложение должно быть авторизовано до начала эксплуатации и повторно авторизовано, по крайней мере, каждые три года после того. Официальное санкционирование подразумевает принятие риска каждой системы, использующей приложение.

4. Присвоение Обязанностей

a. Министерство торговли. Министр торговли должен:

1) Разрабатывать и выпускать соответствующие стандарты и руководства для безопасности чувствительной информации в федеральных компьютерных системах.

2) Пересматривать и обновлять руководства для обучения по компьютерной безопасности и принятой практике компьютерной безопасности с помощью со стороны OPM.

3) Обеспечивать агентства руководящими указаниями для планирования обеспечения безопасности, чтобы помочь в разработке их планов безопасности систем и приложений.

4) Предоставлять агентствам руководящие указания и помощь, как соответствующе, относительно рентабельных мер обеспечения для взаимодействия с другими системами.

5) Координировать работы агентств по реакции на инциденты, чтобы способствовать совместному использованию информации о реакции на инциденты и связанных уязвимостях.

6) Оценивать новые информационные технологии, чтобы оценить их уязвимости безопасности, с технической помощью от Министерства обороны, и информировать Федеральные агентства о таких уязвимостях, как только они становятся известны.

b. Министерство обороны. Министр обороны должен:

1) Обеспечивать соответствующие технические рекомендации и помощь (включая продукты для работы) Министерству торговли.

2) Помогать Министерству торговли в оценке уязвимостей появляющихся информационных технологий.

c. Министерство юстиции. Генеральный прокурор должен:

1) Обеспечивать соответствующие руководящие указания агентствам по законным средствам относительно инцидентов безопасности и путям фиксации и работы с обеспечением правопорядка относительно таких инцидентов.

2) Рассматривать соответствующие судебные иски, когда инциденты безопасности происходят.

d. Управление Служб общего назначения. Руководитель управления служб общего назначения должен:

1) Представлять агентствам руководство по вопросам безопасности, когда они получают оборудование для автоматизированной обработки данных (как определено в разделе 111 (a) (2) из закона о Федеральной собственности и Административных службах 1949, с уточнениями).

2) Облегчать разработку положений контрактов для агентств, для использования при приобретении рентабельных продуктов и услуг безопасности (например, резервных сервисов).

3) Предоставлять соответствующие сервисы безопасности, чтобы удовлетворить потребности Федеральных агентств таким образом, чтобы такие сервисы были рентабельны.

e. Офис Управления персоналом. Директор Офиса Управления персоналом должен:

2) Помогать Министерству торговли в обновлении и поддержании руководящих указаний относительно обучения по компьютерной безопасности и принятой практике компьютерной безопасности.

f. Совет по Политике безопасности. Совет по Политике безопасности должен координировать работы Федерального правительства относительно безопасности информационных технологий, которые обрабатывают классифицированную информацию в соответствии с применимыми директивами национальной безопасности;

5. Исправление недостатков и отчеты

a. Исправление недостатков. Агентства должны исправить недостатки, которые идентифицированы через пересмотры безопасности для систем и главных приложений, описанных выше.

b. Отчеты относительно недостатков. В соответствии с Циркуляром OMB № A-123, "Целевое управление и контроль", если недостаток в мерах безопасности, как оценивает руководитель агентства, является важным в соотношении с другими недостатками агентства, он должен быть включен в ежегодный отчет FMFIA. Менее существенные недостатки должны быть зафиксированы и проведение корректирующих действий должно быть отслежено на соответствующем уровне агентства.

c. Сводки Планов обеспечения безопасности. Агентства должны включать сводку своих планов безопасности систем и планов главных приложения в стратегический план, требуемый законом о Сокращении Документов (44 U.S.C. 3506).

B. Описательная Информация.

Следующий описательный стиль предназначен для объяснения. Это включено, чтобы помочь в понимании требований Приложения.

Приложение переориентирует Федеральную программу компьютерной безопасности, чтобы лучше ответить на быстро изменяющуюся технологическую среду. Оно устанавливает обязанности всего правительства по федеральной компьютерной безопасности и требует, чтобы Федеральные агентства приняли минимальный набор организационных мер безопасности. Эти организационные меры безопасности направлены на отдельных пользователей информационных технологий, чтобы отразить распределенную сущность сегодняшних технологий.

Чтобы безопасность была наиболее эффективной, меры безопасности должны быть частью повседневной деятельности. Это лучше всего выполняется, когда безопасность планируется не как отдельная деятельность, а как неотъемлемая часть всего планирования.

"Адекватная безопасность" определена как " безопасность, соразмерная с риском и величиной вреда, следующего из потери, неправильного употребления или несанкционированного доступа к или модификации информации". Это определение явно подчеркивает основанную на риске политику для рентабельной безопасности, установленную Законом об информационной безопасности.

Приложение больше не требует подготовки формальных анализов рисков. В прошлом существенные ресурсы расходовались на сложные исследования конкретных рисков к системам, с ограниченной материальной выгодой с точки зрения улучшения безопасности для систем. Вместо того чтобы продолжать пытаться точно измерить риск, усилия по безопасности лучше направить на общую оценку рисков и принятие мер по управлению ими. Несмотря на то, что формальные анализы рисков не должны выполняться, необходимость определения адекватной безопасности требует, чтобы использовался основанный на риске подход. Этот подход оценки степени риска должен включать рассмотрение основных факторов в управлении рисками: значение системы или приложения, угрозы, уязвимости и эффективность текущих или предложенных мер защиты. Дополнительное руководство по эффективной оценке степени риска доступно во "Введении в Компьютерную безопасность: Справочник NIST" (16 марта 1995).

Обсуждение раздела Главные Положения. Следующее обсуждение представлено, чтобы помочь рецензентам в понимании изменений в акцентах в разделе.

Программы безопасности автоматизированной информации. Агентства обязаны устанавливать меры, чтобы гарантировать адекватную безопасность для всей информации, которая обрабатывается, передаётся или хранится в федеральных автоматизированных информационных системах. Это Приложение подчеркивает организационные меры безопасности, влияющие на отдельных

пользователей информационной технологии. Технические и эксплуатационные меры безопасности поддерживают организационные меры безопасности. Чтобы быть эффективными, все должны находиться во взаимосвязи. Например, аутентификация отдельных пользователей - важная организационная мера безопасности, для которой защита паролем - техническая мера. Однако защита паролем эффективна будет только если будет использована стойкая технология и ей управляют таким образом, чтобы гарантировать, что она используется правильно.

Определены четыре меры безопасности: возложение ответственности за безопасность, планирование обеспечения безопасности, периодический пересмотр мер безопасности и официальное санкционирование. Приложение требует, чтобы эти организационные меры безопасности были применены в двух областях ответственности за управление: одна для систем общей поддержки и одна для главных приложений.

Термины " система общей поддержки" и "главное приложение" были использованы в Бюллетенях OMB № 88-16 и 90-08. Система общей поддержки - " означают взаимосвязанный набор информационных ресурсов под некоторым прямым административным управлением, которые предоставляют общую функциональность. " Такая система может быть, например, локальной сетью (LAN), включая умные терминалы, которая поддерживает филиалы, обще-агентскую магистраль, систему коммуникаций, ведомственный центр обработки данных, включая его операционную систему и утилиты, тактическую радиосеть, или организацию, обслуживающую обработку совместно используемой информации. Обычно, назначение системы общей поддержки состоит в том, чтобы обеспечить поддержку обработки или коммуникаций.

Главное приложение - использование информации и информационных технологий, чтобы удовлетворить конкретный набор требований пользователя, который требует особого внимания к безопасности вследствие риска и величина вреда, следующего из потери, неправильного употребления или несанкционированного доступа к или модификации информации в приложении. Все приложения требуют некоторого уровня безопасности, и адекватная безопасность для большинства из них должна быть обеспечена безопасностью систем общей поддержки, в которых они работают. Однако, некоторые приложения, из-за сущности информации в них, требуют специального надзора руководства и должны рассматриваться как главные. Агентства, как ожидается, используют решение руководства в определении, какие из их приложений являются главными.

Фокус Бюллетеней OMB № 88-16 и 90-08 сосредоточен на идентификации и обеспечении безопасности и систем общей поддержки и приложений, которые содержат чувствительную информацию. Приложение требует установления мер безопасности во всех системах общей поддержки, исходя из предположения, что все они содержат некоторую чувствительную информацию, и фокусирует дополнительные меры безопасности на ограниченном количестве особенно рискованных или главных приложений.

a. Системы общей поддержки. Следующие меры обеспечения требуются во всех системах общей поддержки:

1) Возложение ответственности за безопасность. Для каждой системы должен быть человек который являлся бы фокусом для того, чтобы гарантировать, что есть адекватная безопасность в пределах системы, включая способы предотвращения, обнаружения и восстановления после решения проблем безопасности. Эта ответственность должна быть возложена в письменной форме на человека, обученного технологии, используемой в системе, и в обеспечении безопасности для такой технологии, включая управление мерами безопасности, такими как идентификация и аутентификация пользователя.

2) План обеспечения безопасности. Закон об информационной безопасности требует, чтобы планы обеспечения безопасности были разработаны для всех федеральных компьютерных систем, которые содержат чувствительную информацию. Учитывая расширение использования распределенной обработки после принятия закона, Приложение исходит из предположения, что все системы общей поддержки содержат некоторую чувствительную информацию, которая требует защиты, чтобы гарантировать их целостность, доступность или конфиденциальность, и, поэтому, все системы требуют планов обеспечения безопасности.

Предыдущее руководство по планированию обеспечения безопасности содержалось в Бюллетене OMB № 90-08. Это Приложение заменяет Бюллетень OMB 90-08 и расширяет охват планов обеспечения безопасности из Бюллетеня 90-08, чтобы включить правила действий людей так же, как и технической безопасности. Непротиворечивое с Бюллетенем OMB 90-08, Приложение предписывает NIST обновить и расширить руководство планирования обеспечения безопасности и выпустить это как стандарт обработки федеральной информации (FIPS). Тем временем, агентства должны продолжать использовать Приложение Бюллетеня OMB № 90-08 как руководство для технической части их планов обеспечения безопасности.

Приложение продолжает требовать, чтобы были получены независимые рекомендации и комментарии в отношении плана обеспечения безопасности для каждой системы. Назначение этого требования состоит в том, чтобы улучшить планы, способствовать взаимодействию между менеджерами различных систем и способствовать совместному использованию экспертизы безопасности.

Это Приложение также продолжает требование из Закона об информационной безопасности о том, что сводки планов обеспечения безопасности должны быть включены в стратегические планы агентства по управлению информационными ресурсами. OMB обеспечит дополнительное разъяснение о содержании этих стратегических планов в соответствии с законом о Сокращении Документов 1995.

Следующие конкретные меры безопасности должны быть включены в планы обеспечения безопасности для систем общей поддержки:

> а) Правила. Важное новое требование для планов обеспечения безопасности - установление ряда правил поведения для отдельных пользователей каждой системы общей поддержки. Эти правила должны ясно очерчивать обязанности и ожидания для всех людей с доступом к системе. Они должны быть непротиворечивыми со специфичной для системы политикой, как описано во "Введении в компьютерную безопасность: Справочник NIST" (16 марта 1995). Кроме того, они должны определять последствия их несоблюдения. Правила должны быть в письменной форме и формировать базис для обучения и освоения безопасности.
>
> Разработка правил для системы должна учитывать потребности всех сторон, которые используют систему. Правила должны быть строгими насколько, насколько необходимо, чтобы обеспечить адекватную безопасность. Поэтому, для системы должен быть установлен допустимый уровень риска и он должен являться основанием для того, чтобы определить правила.
>
> Правила должны закрыть такие вопросы, как работа дома, коммутируемый доступ, соединение с Интернетом, использование произведений, охраняемых авторским правом, неофициальное использование правительственного оборудования,

присвоение и ограничение системных полномочий и индивидуальной подконтрольности. Частично правила должны отразить технические меры безопасности в системе. Например, правила относительно использования пароля, должны быть непротиворечивыми с техническими функциями пароля в системе. Правила могут быть определены через административные санкции, определенным образом связанные с системой (например, потеря системных полномочий) или через более общие санкции, которые накладываются при нарушении других правила проведения. Кроме того, правила должны специально определять восстановление сервиса, как интерес всех пользователей системы.

b) Обучение.

Закон об информационной безопасности требует, чтобы Федеральные агентства предусмотрели обязательное периодическое обучение компьютерной безопасности и принятой практике компьютерной безопасности всех сотрудников, которые связаны с управлением, использованием или эксплуатацией Федеральной компьютерной системы внутри или под контролем Федерального агентства. Это относится к подрядчикам, так же как и к сотрудникам агентства. Доступ, обеспечиваемый для сторонних пользователей, должен быть ограничен мерами безопасности в приложениях через которые предоставляется доступ, и обучение должно быть в пределах контекста этих мер безопасности. Настоящее приложение предписывает проведение обязательного обучения, требуя его завершения до предоставления доступа к системе. Каждый новый пользователь системы общей поддержки в некотором смысле представляет риск для всех других пользователей. Поэтому, каждый пользователь должен быть сведущим в приемлемом поведении - правилах системы - прежде, чем ему будет позволено использовать систему. Обучение должно также информировать человека как получить помощь в случае возникновения трудностей с использованием или безопасностью системы.

Обучение должно быть адаптировано к тому, что пользователь должен знать, чтобы использовать систему безопасно, учитывая сущность такого использования. Обучение может быть представлено по стадиям, например по мере расширения предоставления доступа. В некоторых случаях обучение должно проводиться в форме инструктажа в аудитории. В других случаях, в зависимости от риска и величины вреда, может быть достаточно интерактивных компьютерных сеансов или правильно написанных и понятных брошюр.

С течением времени внимание к безопасности имеет тенденцию рассеиваться. Кроме того, изменения в системе могут требовать изменения в пользовательских процедурах или правилах. Поэтому, люди должны периодически проходить переподготовку, чтобы гарантировать, что они продолжают понимать и соблюдать применимые правила.

Чтобы помочь агентствам, Приложение требует от NIST, с помощью со стороны Офиса Управления персоналом (OPM), обновить его существующее руководство. Оно также предполагает, чтобы OPM гарантируют, что их правила обучения компьютерной безопасности для федеральных гражданских сотрудников являются эффективными.

c) Меры безопасности персонала. В течение долгого времени приходило понимание, что самый большой вред происходит от авторизованных людей, осуществляющих неуместную деятельностью, как преднамеренную так и случайную. В каждой системе

общей поддержки используется много технических, эксплуатационных и организационных мер безопасности, чтобы предотвратить и обнаружить вред. Такие меры безопасности включают индивидуальную подконтрольность, "наименьшее количество полномочий" и разделение обязанностей.

Индивидуальная подконтрольность состоит из возложения на кого-то ответственности за его или её действия. В системе общей поддержки подконтрольность обычно выполняется путем идентификации и аутентификации пользователей системы и впоследствии прослеживания их действий в системе пользователю, который инициировал их. Это может быть сделанное, например, путем обнаружения образцов поведения пользователей.

Наименьшее количество полномочий - практика ограничения доступа пользователя (к файлам с данными, к возможности обработки или к периферийным устройствам) или типа доступа (чтение, запись, выполнение, удаление) до минимума, необходимого, чтобы выполнить его или её задание.

Разделение обязанностей - практика деления шагов в критической функции среди различных людей. Например, один системный программист может создавать критическую часть кода операционной системы, в то время как другой - авторизовать его реализацию. Такая мера обеспечения препятствует отдельному человеку разрушать критический процесс.

Однако, в некоторых случаях, людям могут быть даны возможности обходить некоторые существенные технические и эксплуатационные меры безопасности, чтобы выполнять системное администрирование и функции поддержки (например, администраторам LAN или системным программистам). Контроль таких людей на ответственных постах должен дополнять технические, эксплуатационные и организационные меры безопасности, особенно где риск и величина вреда высоки.

d) Способность реакции на инциденты. Инциденты безопасности, вызванные вирусами, хакерами или программными ошибками, широко распространены. При столкновении с инцидентом безопасности агентство должно быть в состоянии ответить в способе, который и защищает его собственную информацию и помогает защитить информацию других, на которых мог бы влиять инцидент. Чтобы решать эти проблемы, агентства должны установить формальные механизмы реакции на инциденты. Подготовка и обучение для людей с доступом к системе должны включать, как использовать возможности системы по реакции на инциденты.

Чтобы быть полностью эффективной, обработка инцидента должна также включать совместное использование информации относительно общих уязвимостей и угроз в других системах и других агентствах. Приложение нацеливает агентства на то, чтобы осуществлять такое совместное использование, и задача NIST координировать такие обще-правительственные работы агентства.

Приложение также нацеливает Министерство юстиции, чтобы обеспечить соответствующее руководство по законным средствам расследования в случае серьезных инцидентов.

e) Непрерывность поддержки. Неизбежно, будут прерывания сервиса. Планы агентства должны гарантировать, что есть возможность восстановить и предоставить услугу достаточную, чтобы удовлетворить минимальные потребности пользователей системы. Ручные процедуры - обычно НЕ жизнеспособный резервный вариант. Когда автоматизированная поддержка будет не доступна, много функций организации станут не эффективными. Поэтому, важно сделать рентабельные шаги, чтобы управлять любым нарушением сервиса.

Решения об уровне обслуживания, необходимом в любое определённое время и о приоритетах в восстановлении сервиса, должны быть приняты после консультаций с пользователями системы и включены в системные правила. Опыт показал, что планы восстановления, которые периодически тестируются, существенно более жизнеспособны чем те, которые нет. Кроме того, не протестированные планы могут фактически создавать ложное чувство безопасности.

f) Техническая безопасность. Агентства должны гарантировать, что каждая система использует соответствующие эффективные продукты и технологии безопасности, непротиворечивые со стандартами и руководствами от NIST. Часто такие технологии будут соответствовать системным правилам поведения, так как в правильном использовании парольной защиты.

Приложение направляет NIST на продолжение выпуска руководств по компьютерной безопасности, чтобы помочь агентствам в планировании и использовании продуктов и технологий технической безопасности. Однако, пока такое руководство не выпущено, руководство по планированию, включенное в Бюллетень OMB 90-08, может помочь в определении технологий для эффективной безопасности в системе и в применении технических мер безопасности в плане обеспечения безопасности.

g) Взаимосвязь систем. В порядке общности, чтобы эффективно управлять риском, должен контролироваться доступ к и от других систем. Степень такой меры безопасности должна быть установлена в правилах системы и все участники должны знать о любых ограничениях на внешний доступ. Технические меры безопасности, необходимые для выполнения этого, должны быть реализованы в соответствии с руководством, выпущенным NIST.

Есть различные степени того, насколько система взаимодействует. Например, некоторые системы будут предпочитать изолировать себя, другие ограничат доступ, таким, как разрешение соединений только электронной почты или удаленного доступа только со сложной аутентификацией, а другие будут полностью открыты. Управленческое решение по взаимодействию должно быть основано на доступности и использовании технических и нетехнических мер защиты и быть непротиворечивым с допустимым уровнем риска, определенным в системных правилах.

3) Пересмотр мер безопасности. Безопасность системы ухудшается с течением времени, поскольку технологии развиваются и как следствие изменения процедур и людей. Пересмотры должны гарантировать, что организационные, эксплуатационные, управления персоналом и технические меры безопасности функционирует эффективно. Меры безопасности могут быть пересмотрены независимым аудитором или самостоятельно. Тип и строгость пересмотра или аудита должны быть соразмерны с допустимым уровнем риска, который установлен в правилах для системы и возможности изучения полезной информации, чтобы улучшить

безопасность. Технические инструменты, такие как вирусные сканеры, продукты оценки уязвимости (которые ищут известные проблемы безопасности, ошибки конфигурации и установку последних патчей) и тестирование на возможность проникновения могут помочь в постоянном анализе различных аспектов систем. Однако, эти инструменты - не замена для формального управленческого пересмотра, по крайней мере, каждые три года. Более того, для некоторых рискованных систем с быстро изменяющейся технологией, три года будут слишком долгими.

В зависимости от риска и величины вреда, которые могут быть результатом, о слабых местах, идентифицированных во время пересмотра мер безопасности, необходимо сообщить как о недостатках в соответствии с Циркуляром OMB № A-123, "Целевое управление и контроль" и Федеральным законом о менеджерах финансовый целостности. В частности, если основные организационные меры безопасности такие, как присвоение ответственности, осуществляемый план обеспечения безопасности или управленческое санкционирование отсутствуют, то внимание должно быть сосредоточено на идентификации недостатков.

4) Санкционирование на обработку. Санкционирование обработки в системе информации, предоставленное официальным должностным лицом руководства, обеспечивает важный контроль качества (некоторые агентства именуют это санкционирование как аттестацию). Санкционируя обработку в системе, менеджер принимает риск, связанный с этим. Санкционирование - решение, которое должно быть принято не службой безопасности.

И у сотрудника службы безопасности и у санкционирующего должностного лица руководства есть обязанности по безопасности. Вообще, сотрудник службы безопасности ближе к повседневной эксплуатации системы и организует или выполняет задачи безопасности. Санкционирующее должностное лицо обычно несёт общую ответственность за организационную поддержку системы.

Санкционирование руководством должно быть основано на оценке организационных, эксплуатационных и технических мер безопасности. Так как план обеспечения безопасности устанавливает меры безопасности, он должен формировать основание для санкционирования, дополненное более конкретными исследованиями при необходимости. Кроме того, периодический пересмотр мер безопасности должен также способствовать будущему санкционированию. Некоторые агентства периодически выполняют "аттестационные испытания" их систем. Эти формальные технические оценки приводят к аттестации системы руководством или к "санкционированию на обработку." Эти аттестационные испытания (такие как те, которые используют методологию в FIPS Pub 102 "Руководство по аттестационным испытаниям компьютерной безопасности и аттестации"), могут обеспечить полезную информацию, чтобы помочь руководству в санкционировании системы, особенно когда это объединено с пересмотром общих поведенческих мер безопасности, предполагаемых в плане обеспечения безопасности, требуемом Приложением.

Пересанкционирование должно происходить до существенного изменения в процессе обработки, но, по крайней мере, каждые три года. Это должно делаться чаще там, где есть высокий риск и потенциальная величина вреда.

b. Меры безопасности в Главных приложениях. Некоторые приложения требуют специального внимания руководства вследствие риска и величина вреда, которые могут произойти. Для таких приложений меры безопасности системы(м) поддержки, в которой они работают, вероятно будут недостаточны. Поэтому, требуются дополнительные меры

безопасности, конкретные к приложению. Так как функция приложений - непосредственное управление и использование информации, меры для того, чтобы обеспечить безопасность приложения должны подчеркнуть защиту информации и способа, которым этим манипулировать.

1) Возложение ответственности за безопасность. По определению, главные приложения являются высоко рисковыми и требуют специального внимания руководства. Главные приложения обычно поддерживают отдельную функцию агентства и часто поддерживают более чем одну систему общей поддержки. Важно, поэтому, что бы на человека была в письменной форме возложена ответственность чтобы гарантировать, что у определенного приложения есть адекватная безопасность. Чтобы это было эффективным, этот человек должен быть хорошо осведомлен в информации и процессе, поддерживаемых приложением, и в организационных, управления персоналом, эксплуатационных и технических мерах безопасности, использованных для защиты приложения.

2) Планы Безопасности приложений. Безопасность для каждого главного приложения должна определяться планом обеспечения безопасности, конкретным для приложения. План должен включать меры, определенные для защиты информации, и должен быть разработан из перспективы применения приложения. Чтобы получить уверенность в его жизнеспособности, план должен быть предоставлен для рекомендаций и комментариев менеджеру системы общей поддержки, которая использует приложение. Этим признается критическая зависимость безопасности главных приложений для базовых систем поддержки, в которых они используются. Сводки планов безопасности приложений должны быть включены в стратегические планы управления информационными ресурсами в соответствии с этим Циркуляром.

a) Правила приложения. Должны быть установлены правила поведения, которые ясно очерчивают обязанности и ожидаемое поведение всех людей с доступом к приложению. Правила должны определять последствия их несоблюдения. Часто правила будут связаны с техническими мерами безопасности, реализованными в приложении. Такие правила должны включать, например, ограничения на изменение данные, поиск в базах данных или разглашение информации.

b) Специализированное обучение. Обучение требуется для всех людей, которым предоставляют доступ к приложению, включая публичных пользователей. Оно должно меняться в зависимости от типа предоставленного доступа и риска, который представляет доступ для безопасности приложения и информации в нем. Это обучение будет в дополнение к требуемому для доступа к системе поддержки.

c) Безопасность персонала. Для большинства главных приложений, организационные меры безопасности, такие как требования индивидуальной подконтрольности, разделение режимов работы, определенное мерами контроля доступа или ограничения для людей на полномочия по обработке, является обычно более рентабельными мерами безопасности персонала чем фоновый контроль. Такие меры безопасности должны быть реализованы и как технические меры и как правила для приложения. Например, технические меры чтобы гарантировать индивидуальную подконтрольность, такие как поиск образцов пользовательского поведения, являются самыми эффективными если пользователи знают, что есть такие технические меры. Если адекватные меры аудита или контроля доступа (и через технические и через нетехнические методы) не могут быть установлены, то может быть рентабельным контролировать персонал, соразмерно с величиной риска и вреда, которые они могут вызвать. Изменение в акценте на контроль в Приложении не должно влиять на

фоновый контроль, который считается необходимым из-за других режимов работы, которые может выполнять человек.

d) Планирование на случай непредвиденных ситуаций. Обычно выполнение федерального предназначения, поддерживаемого главным приложением, критически зависит от приложения. Ручная обработка - обычно НЕ жизнеспособный резервный вариант. Руководство должно планировать то, как оно будет выполнять свое предназначение и/или восстановление с потери существующей поддержки приложения, является ли потеря следствием неспособности приложения функционировать или отказом системы общий поддержки. Опыт показал, что тестирование плана действий при непредвиденных обстоятельствах значительно улучшает его жизнеспособность. Действительно, не протестированные планы или планы, не протестированные в течение длительного периода времени, могут создать ложное чувство возможности восстановиться своевременно.

e) Технические меры. Технические меры безопасности, например тесты по фильтрации недопустимых записей, должны быть встроены в каждое приложение. Часто эти меры безопасности будут соответствовать правилам поведения для приложения. В соответствии с предыдущим Приложением, безопасность приложений фокусировалась на процессе, в соответствии с которым были разработаны чувствительные прикладные программы. Несмотря на то, что этот процесс не рассматривается подробно в этом Приложении, он остается эффективным методом для того, чтобы гарантировать, что меры безопасности встроены в приложения. Дополнительно, технические меры безопасности, определенные в Бюллетене OMB № 90-08, будут продолжать действовать, пока это руководство не будет заменено руководством планирования обеспечения безопасности NIST.

f) Совместное использование информации. Гарантируйте, что информация, которой делятся с Федеральными организациями, правительствами штатов и местными органами власти и частным сектором, соответственно защищена сопоставимо с защитой, обеспечиваемой когда информация находится в пределах приложения. Меры безопасности информации могут остаться теми же самыми или изменяться, когда информацией делятся с другой сущностью. Например, для основного пользователя информации может потребоваться высокий уровень доступности, в то время как вторичного пользователя нет, и поэтому могут быть ослаблены некоторые из мер безопасности, разработанных, чтобы обеспечивать доступность информации. В то же время, однако, передаваемая информация может потребовать уровня конфиденциальности, который должен быть расширен для вторичного пользователя. Это обычно требует уведомления и соглашения по защите информации до того, как она будет совместно использована.

g) Меры обеспечения открытого доступа. Разрешение открытого доступа к федеральному приложению является важным методом улучшения информационного обмена с обществом. Одновременно, это представляет риски федеральному приложению. Чтобы смягчить эти риски, должны быть приняты соответствующие дополнительные меры безопасности. Эти меры безопасности должны быть приняты в дополнение к таким мерам, как "межсетевой экраны", которые положены для безопасности системы общей поддержки.

Вообще, к системам открытого доступа более трудно применить стандартные меры безопасности, потому что многие из пользователей системы могут быть не подчиненными отдельным политикам подконтрольности. Кроме того, системы открытого доступа могут быть объектами для нанесения вреда из-за их более высокой видимости и опубликованных методов доступа.

Официальные документы должны быть защищены от потери или изменения. Официальные документы в электронной форме особенно восприимчивы, так как их можно относительно легко изменить или уничтожить. Поэтому, официальные документы должны быть отделены от информации, являющейся непосредственно доступной обществу. Есть различные способы выделять записи. Некоторые агентства и организации создают выделенные информационные системы распространения (такие как доски объявлений или серверы всемирной паутины), чтобы поддержать эту функцию. Эти системы могут быть за пределами безопасных шлюзов, которые защищают внутренние записи агентства от внешнего доступа.

Чтобы обеспечить безопасность приложений, которые позволяют прямой открытый доступ, должны также использоваться стандартные технологии такие, как наименьшее количество полномочий (ограничение способности обработки так же как доступа к данным) и доверие к целостности (такое как проверка на вирусы, явное маркирование срока данных или периодическая проверка изменения данных). Дополнительное разъяснение по обеспечению безопасности систем открытого доступа доступно в бюллетене Лаборатории Компьютерных систем NIST «Аспекты безопасности в системах открытого доступа" (май 1993).

3) Пересмотр мер безопасности приложения. По крайней мере каждые три года должны быть выполнены независимый пересмотр или аудит мер безопасности для каждого главного приложения. Из-за более высокого риска, связанного с главными приложениями, пересмотр или аудит должны быть независимыми от менеджера, ответственного за приложение. Такие пересмотры должны подтверждать, что ответственность за безопасность приложения была возложена, что для приложения имеется жизнеспособный план обеспечения безопасности и что менеджер санкционировал обработку приложения. Недостаток в любой из этих мер безопасности нужно считать недостатком в соответствии с законом о федеральных менеджерах финансовой целостности и Циркуляром OMB № A-123, "Целевое управление и контроль".

Предполагаемый здесь пересмотр отличается от испытаний системы и аттестации, требуемых в настоящем Приложении. Указанный процесс, однако, остается полезным для убеждения в том, что технические средства защиты встроены в разработанные для пользователей программные приложения. В то время как меры безопасности в указанном процессе не требуются определенно в этом Приложении, они остаются в Бюллетене № 90-08 и рекомендуются при соответствующих обстоятельствах как технические меры безопасности.

4) Санкционирование обработки. Главное приложение должно быть санкционировано официальным должностным лицом, официальным ответственным за функцию, поддерживаемую приложением по крайней мере каждые три года, но возможно чаще там, где риск и величина вреда высоки. Назначение этого требования состоит в том, чтобы гарантировать, что высшее должностное лицо, на предназначение которого

оказывают негативное влияние слабые места безопасности в приложении, периодически оценивает и принимает риск применения приложения. Санкционирование должно быть основано на плане безопасности приложения и любой проверке (ах), выполненной в отношении приложения. Он должно также принять во внимание риски от систем общей поддержки, используемых приложением.

4. Присвоение обязанностей. Приложение возлагает те обще-правительственные обязанности на агентства, которые непротиворечивы с их предназначением и Законом об информационной безопасности.

a. Министерство торговли. На Министерство торговли, через NIST, возложены следующие обязанности, непротиворечивые с Законом об информационной безопасности.

1) Разработка и выпуск стандартов обеспечения безопасности и руководств.

2) Пересмотр и обновление, с помощью со стороны OPM, руководств по обучению безопасности выпущенных в 1988 г. в соответствии с Законом об информационной безопасности, чтобы гарантировать, что они эффективны.

3) Замена и обновление руководства по техническому планированию, являющегося приложением к Бюллетеню OMB 90-08. Оно должно включать руководство по эффективной, основанной на риске безопасности, с исключением формального анализа рисков.

4) Предоставление агентствам руководства и помощи относительно эффективных мер безопасности для систем, соединенных с другими системами, включая Интернет. Такое руководство по, например, так называемым "межсетевым экранам", становятся широко востребованными и критическими по отношению к агентствам, когда они рассматривают, как соединить их коммуникационные возможности.

5) Координация работы агентств по реакции на инциденты. Координация работ агентств по реакции на инциденты должна быть направлена на угрозы уязвимости и улучшать возможности Федерального правительства по быстрой и эффективной кооперации в ответ на серьезные нарушения защиты.

6) Оценка уязвимостей безопасности в новых информационных технологиях и информирование Федеральных агентств о таких уязвимостях. Назначение этого нового требования состоит в том, чтобы помочь агентствам понять последствия безопасности технологии прежде, чем они купят и применят их. В прошлом было слишком много случаев, когда агентства получали и реализовывали технологию, затем узнавали об уязвимостях в технологии и должны были настраивать меры безопасности. Эта работа предназначена, чтобы помочь избежать таких трудностей в будущем.

b. Министерство обороны. Министерство, через Агентство национальной безопасности, должно обеспечить технический совет и помощь NIST, включая законченные продукты такие как технические руководства по безопасности, которые NIST может использовать для разработки стандартов и руководств по защитите чувствительной информации в федеральных компьютерах.

Кроме того, Министерство, через Агентство национальной безопасности, должен помочь NIST в оценке уязвимостей в появляющихся технологиях. Такие уязвимости могут представить риск информации национальной безопасности, а так же несекретной информации.

c. Министерство юстиции. Министерство юстиции должно обеспечить соответствующее руководство Федеральным агентствам по законным средствам, доступным им, когда серьезные инциденты безопасности происходят. Такое руководство должно включать способы протоколирования инцидентов и взаимодействия с силами обеспечения правопорядка.

Кроме того, Министерство должно сопровождать соответствующие судебные иски от имени Федерального правительства, когда серьезные инциденты безопасности происходят.

d. Управление служб общего назначения. Управление служб общего назначения должно обеспечить руководство агентствами по рассмотрению безопасности при получении продуктов или услуг информационных технологий. Это подтверждает существующее требование.

Кроме того, там где это рентабельно, GSA должно применять для агентств механизмы обще-правительственных контрактов, чтобы использовать для получения некоторых сервисов безопасности. Такие механизмы уже существуют для того, чтобы оказывать поддержку резервирования систем и проводить исследования безопасности.

GSA должно также предоставить соответствующие сервисы безопасности, чтобы помочь Федеральным агентствам до такой степени, чтобы применение таких сервисов было рентабельно. Это включает предоставлении, совместно с Министерством обороны и Министерством торговли, соответствующих сервисов, которые поддерживают федеральное использование Национальной Информационной инфраструктуры (например, использование технологии цифровой подписи).

e. Офис Управления персоналом. В соответствии с Законом об информационной безопасности, OPM должен пересмотреть свое руководящие указания относительно обучения компьютерной безопасности и гарантировать, что они эффективны.

Кроме того, OPM должен помочь Министерству торговли в пересмотре и обновлении его руководящих принципов освоения и обучения компьютерной безопасности. OPM работал в тесном сотрудничестве с NIST в разработке текущих руководящих принципов и должен работать с NIST в пересмотре этих руководящих принципов.

f. Совет по политике безопасности. На Совет по политике безопасности возложена ответственность за координацию политики национальной безопасности в соответствии с соответствующей Президентской директивой. Это включает политику безопасности информационных технологий, используемых для обработки секретных данных.

Циркуляр A-130 и это Приложение действительно не применяются к информационным технологиям, которые поддерживают некоторые критические задачи национальной безопасности, как определено в 44 U.S.C. 3502 (9) и 10 U.S.C. 2315. Политика и процедурные требования для безопасности систем национальной безопасности (телекоммуникации и информационные системы, которые содержат секретные данные или которые поддерживают эти критические задачи национальной безопасности (44 U.S.C. 3502 (9) и 10 U.S.C. 2315)) присвоены Министерству обороны в соответствии с Президентской директивой. Циркуляр разъясняет, что информация, классифицированная как предназначенная для национальной безопасности, должна также быть обработана в соответствии с соответствующими директивами национальной безопасности. Там где секретные данные обязаны быть защищены более строгими требованиями безопасности, должны применяться эти требования, а не требования настоящего Приложения.

5. Отчеты. Приложение требует, чтобы агентства представляли два отчета для OMB:

Первым является требование, что агентства представляют отчет о недостатках безопасности и материалы слабых мест в вместе с их механизмами создание отчетов FMFIA как определено Циркуляром OMB № A-123, "Подконтрольность управления и Мера обеспечения," и принимают меры по ликвидации последствий в соответствии с той директивой.

Вторым, определенным Законом об информационной безопасности, является требование, чтобы сводка планов обеспечения безопасности агентства была включена в информационный план управления ресурсами, который требуется в соответствии с законом о Сокращении Документов.