NIST Special Publication 800-175A

米国連邦政府での暗号標準利用のためのガイドライン：

指令、命令、及び方針

Elaine Barker
William C. Barker

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-175A

コンピュータ セキュリティ

National Institute of Standards and Technology
U.S. Department of Commerce

この文書は以下の団体によって翻訳監修されています

IPA 独立行政法人 情報処理推進機構
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

NIST Special Publication 800-175A

米国連邦政府での暗号標準利用のためのガイドライン：

指令、命令、及び方針

Elaine Barker
コンピュータセキュリティ部門
情報技術研究所

William C. Barker
国内客員研究員
情報技術研究所

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-175A

August 2016

米国商務省
Penny Pritzker、*長官*

米国国立標準技術研究所
Willie May、*NIST 標準技術局長兼商務次官*

発行機関

本文書は、米国国立標準技術研究所（NIST：National Institute of Standards and Technology）によって、2014 年連邦情報セキュリティ近代化法（Federal Information Security Modernization Act (FISMA) of 2014）、合衆国法典（U.S. Code）第 44 編第 3541 条等、公法（P.L.）113-283 に基づく法的責任を推進するために策定された。NIST は、連邦情報システムの最小限の要求事項を含め情報セキュリティ標準及びガイドラインを開発する責務があるが、これらの標準及びガイドラインは、国家安全保障システムについての政策的権限を有する適切な連邦機関の明示的な承認を得ることなしには、国家安全保障システムに適用されてはならない。このガイドラインは、行政管理予算局（OMB：Office of Management and Budget）による通達（Circular）A-130 の要求事項に一致している。

本出版物における一切は、商務長官が法的権威に基づき連邦政府に対して義務及び拘束力を与えた標準及びガイドラインを否定するものではない。また、これらのガイドラインは、商務長官、行政管理予算局長、又は他の全ての連邦政府当局者の既存の権威に変更を加えたり、これらに取って代わったりするものと解釈すべきではない。本出版物は、非政府組織が自由意思で使用することもでき、米国における著作権の制約はないが、NIST に帰属する。

National Institute of Standards and Technology Special Publication 800-175A
Natl. Inst. Stand. Technol. Spec. Publ. 800-175A, 37 pages (August 2016)
CODEN: NSPUE2

本出版物は、以下から無料で利用可能である：
http://dx.doi.org/10.6028/NIST.SP.800-175A

本文書中で特定される商業的組織、装置、又は資料は、実験手順又は概念を適切に説明するためのものである。このような特定は、NIST による推奨又は同意を意味するものではなく、これらの組織、資料、又は装置が、その目的のために利用可能な最善なものであることを意味しているわけでもない。

与えられた法的責任に従い、NIST によって現在作成中のその他の文書への参照が本文書にあるかもしれない。本文書におけるその情報は、概念及び方法論を含め、このような関連文書の完成前であっても連邦政府機関によって利用されるかもしれない。したがって、それぞれの文書が完成されるまで、現在の要求事項、ガイドライン、及び手順が、存在する限り、運用の効力を有する。計画及び移行目的に関して、連邦政府機関は、NIST によるこれらの新しい文書の開発に密接に従うことを希望するかもしれない。

組織は、パブリックコメント期間中の全てのドラフト文書をレビューし、NIST へフィードバックを提供するよう奨励する。上記以外の多くの NIST サイバーセキュリティ文書は、http://csrc.nist.gov/publications から入手可能である。

本出版物へのコメントは以下で受け付ける：

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive（Mail Stop 8930）Gaithersburg, MD 20899-8930
Email: SP800-175@nist.gov

全てのコメントは、連邦情報公開法（FOIA）の下での公開対象である。

コンピュータシステムの技術に関する報告書

米国国立標準技術研究所（NIST：National Institute of Standards and Technology）情報技術研究所（ITL：Information Technology Laboratory）は、国家の計測及び標準に関する基盤において技術的リーダーシップを提供することにより、米国の経済及び社会福祉に貢献している。ITL は、テスト、テスト技法、参照データ、概念実証及び技術的分析の開発を通じて、情報技術の開発と生産的利用の発展に努めている。ITL の責務は、連邦政府の情報システムにおいて、国家安全保障に関連する情報以外の情報に対する費用対効果の高いセキュリティとプライバシーを実現するための、管理面、運用面、技術面及び物理面での標準及びガイドラインを策定することを含んでいる。本 Special Publication 800 シリーズは、情報システムセキュリティに関する ITL の調査、ガイドライン及び普及活動、ならびに産業界、政府機関及び学術機関との共同活動について報告する。

要旨

本文書は、デジタル化された機密ではない機微情報を送信中及び保管中に保護するために暗号技術及び NIST の暗号標準を使用する際のガイダンスを連邦政府に提供することを目的としたシリーズの一部である。Special Publication (SP) 800-175A は、暗号を使用するための要件の決定に関するガイダンスを提供する。これには、連邦政府の機微情報の保護に関する法律及び規則の概要、保護すべき対象とその情報を保護するための最善の方法を決定するためのリスクアセスメントの実施に関するガイダンス、及び関係するセキュリティ関連文書（様々なポリシーや実践文書など）の説明が含まれる。

キーワード

認証； 機密性； 重要インフラ； 暗号ガイドライン； 暗号技術； 大統領令； 完全性； 鍵管理； 法律； 命令； 方針； 大統領指令； リスクアセスメント； 標準

謝辞

本文書の元となった NIST Special Publication (SP) 800-21 の著者である Annabelle Lee 氏をはじめ、本文書のドラフトをレビューし、その開発に貢献してくれた同僚に感謝したい。また、公的機関ならびに民間の方々による、本刊行物の品質及び有用性を向上させる思慮深く建設的なコメントをいただいたことにも深く感謝の意を表する。

特許公開の通知

通知：情報技術研究所（ITL）は、本書のガイダンスや要件に準拠するために使用が必要となる可能性のある特許請求項の所有者に対し、その特許請求項を ITL に開示するよう要請している。しかし、特許保有者は ITL の特許募集に応じる義務はなく、ITL は本書に適用される特許があるとしても、それを特定するための特許調査を行っていない。

本書を発行し、本書のガイダンスや要件に準拠するために使用が必要となる可能性のある特許請求項を特定するための呼びかけを行った時点で、ITL はそのような特許請求項を特定していない。

ITL は、本書の使用において特許侵害を回避するためのライセンスが必要ないことを表明又は暗示するものではない。

本文書は、原典に沿ってできるだけ忠実に翻訳するよう努めていますが、完全性、正確性を保証するものではありません。翻訳監修主体は、本文書に記載されている情報より生じる損失又は損害に対して、いかなる人物あるいは団体についても責任を負うものではありません。

目次

1 はじめに 1

1.1 背景と目的 1

1.2 用語と定義 1

1.3 頭字語 4

1.4 文書構成 5

2 適用可能な公法 6

2.1 2002 年電子政府法（FISMA） 6

2.2 経済的及び臨床的健全性のための医療情報技術に関する法律（HITECH） 7

2.3 2014 年連邦政府情報システム近代化法 8

2.4 2014 年サイバーセキュリティ強化法 9

3 大統領行政府指令 11

3.1 国家安全保障大統領指令第 7 号（HSPD-7）：重要インフラの特定、優先順位付け、及び保護 11

3.2 HSPD-12: 連邦政府職員ならびに請負業者の共通 ID 標準指針 11

3.3 大統領令第 13636 号：重要インフラのサイバーセキュリティ改善 11

3.4 OMB 回覧 A-119：自発的な合意標準の制定と利用及び適合性評価活動への連邦政府の参加 12

3.5 OMB 回覧（Circular）A-130：戦略資源としての情報管理 13

3.5.1 プライバシー及び情報セキュリティ条項 13

3.5.2 電子署名条項 14

3.5.3 政府全体としての責任 14

3.5.4 連邦政府情報資源の保護及び管理のための一般要件 15

3.5.5 連邦政府情報リソースの保護及び管理のための具体的要件 15

3.5.6 回覧 A-130 で引用されている NIST ドキュメント 19

3.6 OMB 通知文書（Memorandum）M-06-16：組織の機微情報保護 20

3.7 OMB 通知文書 M-06-18：HSPD-12 実装のための製品とサービスの入手 21

3.8 OMB 通知文書 M-07-16：個人識別情報漏えいに対する防止策及び対応 21

3.9 OMB 通知文書 M-08-23：連邦政府ドメインネームシステム（DNS）基盤の安全性確保 22

3.10 OMB 通知文書 M-11-33：2011 年連邦政府情報セキュリティ管理法及び機関によるプライバシー管理に関する報告指示 23

3.11 OMB 通知文書 M-16-03：2015-2016 年連邦政府情報セキュリティ及びプライバシー管理要求事項に関するガイダンス 25

4 組織的方針 26

4.1 情報管理方針 26

4.2 情報セキュリティ方針 26

4.3 鍵管理方針 26

5　リスクマネジメント手順 28
5.1　情報及び情報システムの分類 28
5.2　セキュリティコントロールの選定 29
付録 A：参考文献 30

1 はじめに

1.1 背景と目的

アメリカ国立標準技術研究所（NIST）発行の暗号化に関する出版物は、暗号技術の活用法に関する指針は記してあるが、いつどのような場面で暗号化が必要かという件に関する記載はない。暗号化による保護を活用するか否かは保護する情報の所有者の判断に任されている。暗号化による保護活用の判断は一般的に、伝送時及び保管時における、保護される情報の機微度合いと、情報を保護するために求められるセキュリティコントロールを定める詳細なリスク分析により決定する。本文書は暗号化を活用する際の要求を定める際の基本となるガイダンスを示す。これには、連邦政府の機密扱いになっていない機微情報の保護に関する法律、指令、標準、ガイドラインの概要を含む；どのような情報を保護する必要があり、かつ、どのように保護するのが最適か判断するためのリスクアセスメント実施ガイド、及び、アプリケーションに関連するセキュリティ文書についての議論（例：様々な方針や実践文書）。連邦政府外での本ガイドラインの活用は完全に任意であるが、本文書に記されているプロセスや参考文献の多くは連邦政府外の活用においても有用である。

連邦暗号化システムに適用される基本的ポリシ文書は、公法（Public Laws）、大統領令（Presidential Executive Orders）や指令（Directives）、及び大統領行政府（Executive Office of the President）から出されたその他のガイダンスを包含する。商務省と NIST の出版物には、連邦政府組織にとって必須の政策文書と認識されているものがある。該当する NIST の暗号化に関する出版物は Special Publication (SP) 800-175B－*米国連邦政府での暗号標準利用のためのガイドライン：暗号化の仕組み*（*Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms*）－の中に記されている。

1.2 用語と定義

Authentication 認証	この文書で用いられる限り、通信や保管される情報の情報源及び完全性の保証、又はエンティティの ID 保証を提供するプロセス
Authorization 認可	情報システムの運用を認可し、合意された一連のセキュリティ対策の実施に基づいて、組織の運営と資産、個人、他の組織、及び国家に対するリスクを明確に受け入れるために、上部組織が下す正式な管理上の決定
Breach 違反	コントロール喪失、危殆化、無認可開示、不正取得、不正アクセス、もしくは類する表現で、認可されていない利用者又は認可されている目的以外の行為をしようとする認可された利用者が、機微情報にアクセスもしくはアクセスの可能性のある行為を物理的又は電子的に行うこと
Categorization 分類	情報又は情報システムのセキュリティ区分を定義するプロセス。セキュリティ分類手法は、国家安全保障システムにおいては CNSS 命令（Instruction）1253 に記されており、それ以外のものについては FIPS 199 に記されている。
Ciphertext 暗号文	暗号化された状態のデータ
Confidentiality 機密性	機微情報が認可されていないエンティティに開示されない性質

Critical Infrastructure 重要インフラ	社会を支える基本的なサービスで、社会の経済、安全と健康を保つ基礎となるもの
Cryptographic algorithm 暗号アルゴリズム	暗号鍵（存在する場合）を含む可変の入力を受け取って出力を生成する明確に定義された計算手順
Cryptographic Key 暗号鍵	暗号アルゴリズムと一緒に使用されるパラメータで、鍵を知っているエンティティは操作を再現もしくは逆演算することができるが、鍵を知らないエンティティはその操作を再現できないように決定づける
Cryptography 暗号／暗号技術	情報を隠ぺい及び検証する方法。安全に、また安定的に機微情報への認可されていないアクセスを抑制したり、確認を可能にしたりするプロトコル、アルゴリズム、手法を含む。主な目的は、機密性、完全性、情報源認証を含む
Digital Infrastructure デジタルインフラ	デジタルインフラは、中央に集中した通信システムを介してデータを保管したり交換したりすることを可能にすることと定義する。データ通信や交換はそのための適切なソフトウェアやハードウェア機器を用いてすべて簡単に行えるようになっている
Encryption 暗号化	セキュリティとプライバシーを守るために平文を暗号文に変更するプロセス
Entity エンティティ	個人（人）、組織、デバイスもしくはプロセス
Executive Office of the President 大統領行政府	大統領直属のスタッフで、行政管理予算局、国家安全保障スタッフ、科学技術政策局、人事管理局などのエンティティを伴う
Executive Orders 大統領令	行政機関の長として連邦行政機関に対して大統領から発せられる法廷拘束力を持つ指示。通常は連邦政府組織や職員に対して議会で成立した法や方針の実行を命ずる際に発せられる
High Impact 高インパクト	機密性、完全性、もしくは可用性の喪失が、組織運営や組織の資産、もしくは個人に対して重篤な大惨事に招きかねない状況
Identity Management ID 管理	広くはシステム内で個々を特定するための管理のことで、特定の会社内やネットワーク内、国といった単位で行う。企業 IT での ID 管理は、個々のネットワークユーザの役割やアクセス権限を与え管理することを示す
Integrity 完全性	保護されたデータが不正かつ検知されない方法で変更又は削除されていない性質
Key Establishment 鍵確立	異なる関係者間で共有する鍵材料を生成する手順
Keying Material 鍵材料	暗号鍵関係を構築・維持する必要のあるデータ（例：鍵）

Key Management 鍵管理	The activities involving the handling of cryptographic keys and other related security parameters (e.g., counters) during the entire life cycle of the keys, including the generation, storage, establishment, entry and output, and destruction. 生成、保管、確立、入出力、及び破棄など、鍵のライフサイクル全体にわたり、暗号鍵及びその他の関連するセキュリティパラメータ（例えば、カウンタ）の取扱いに関わるアクティビティ
Low-Impact 低インパクト	機密性、完全性、もしくは可用性の喪失が、組織運営や組織の資産、もしくは個人に対して限定的な悪影響しか与えないと予想される状況
Mandate 命令	法規の下、必須の指示又は要求事項
Moderate Impact 中インパクト	機密性、完全性、もしくは可用性の喪失が、組織運営や組織の資産、もしくは個人に対して重大な不利益を与える可能性がある状況
Plaintext 平文	暗号化アプリケーションを使用することなく意味があり理解できる明瞭なデータ
Policy 方針／ポリシ	ガイドラインを伴う基本原則群で、長期目標に至るための行動を指導し制限するために組織内の統制部隊によって作成及び施行されたもの
Presidential Directive 大統領指令	アメリカ国家安全保障会議のアドバイスと了承を得てアメリカ大統領が発する行政命令。大統領決定指令とも呼ぶ。
Reciprocity 互恵主義	参加組織間で、情報システム資源の相互利用ために互いのセキュリティ評価の受け入れや、情報共有のための互いの評価済みのセキュリティ制度の受け入れを行うことを相互承認すること
Risk Analysis リスク分析	リスク評価を参照のこと
Risk Assessment リスク評価	情報システムの運用に伴う組織運営（例えば、ミッション、機能、イメージ、評判など）、組織資産、個人、他の組織、及び国家に対するリスクを特定するプロセス。リスク管理の一部であり、脅威及び脆弱性の分析を組み込み、計画又は実施されているセキュリティ対策によって提供される緩和策を検討する。
Risk Management リスク管理	組織運営（例えば、ミッション、機能、イメージ、評判など）、組織資産、個人、他の組織、国家に対する情報セキュリティリスクを管理するためのプログラムとそれを支えるプロセスであり、以下を含む：(i) リスク関連活動の状況確立、(ii) リスク評価、(iii) 判明したリスクへの対処、及び (iv) 長期間のリスク監視
Security Control セキュリティコントロール	情報の機密性、完全性、及び可用性を保護し、規定されたセキュリティ要件一式に適合するように設計された情報システム又は組織に対して予め規定された予防策もしくは代替策
Security Policy セキュリティ方針	セキュリティサービスを提供するための一連の基準

Security Strength セキュリティ強度	暗号アルゴリズム又はシステムを破るために必要な作業量（操作数）を基準とした強度
Standard 標準／標準規格	要件、仕様、ガイドライン、又は特徴を示す文書であって、材料、商品、プロセスやサービスがその目的に対して常に適合していることを保証することに使われるもの
Two-Factor Authentication 二要素認証	所有している物理的又はソフトウェア的なトークンと記憶している秘密知識との組み合わせで認証すること

1.3 頭字語

CIO	Chief Information Officer（上級情報責任者）
CNSS	Committee for National Security Systems（国家セキュリティシステム委員会）
DHS	Department of Homeland Security（国土安全保障省）
DNSSEC	Domain Name System Security Extensions（ドメインネームシステムセキュリティ拡張）
DOD	Department of Defense（国防総省）
EOP	Executive Office of the President（大統領行政府）
FIPS	Federal Information Processing Standard（連邦情報処理標準）
FISMA	Federal Information Security Management Act (P.L. 107-347)（連邦政府情報セキュリティ管理法（P.L. 107-347)）
GSA	General Services Administration（共通役務庁／一般調達局）
HHS	Health and Human Services（連邦厚生省）
HIPAA	Health Insurance Portability and Accountability Act（健康保険ポータビリティ及び説明責任法）
HITECH	Health Information Technology for Economic and Clinical Health（経済的及び臨床的健全性のための医療情報技術）
HSPD	Homeland Security Presidential Directive（国家安全保障大統領指令）
IC	Intelligence Community（インテリジェンスコミュニティ）
IG	Inspector General（統括監査官）
IT	Information Technology（情報技術）
ITL	Information Technology Laboratory（情報技術研究所）
JTFTI	Joint Task Force Transformation Initiative
NIST	National Institute of Standards and Technology（国立標準技術研究所）
NISTIR	NIST Interagency or Internal Report（NIST 機関内部報告書）

NPIVP	NIST Personal Identity Verification Program（NIST 個人 ID 認証プログラム）
NSC	National Security Council（国家安全保障会議）
ODNI	Office of the Director of National Intelligence（国家情報長官官房）
OMB	Office of Management and Budget（行政管理予算局）
OPM	Office of Personnel Management（人事管理局）
PHI	Protected Health Information（健康保護情報）
PIV	Personal Identity Verification（個人 ID 認証）
PKI	Public Key Infrastructure（公開鍵基盤）
P.L.	Public Law（公法）
SAOP	Senior Agency Official for Privacy（上級プライバシー責任者）
SP	Special Publication（特別刊行物）
U.S.C.	United States Code（合衆国法典）

1.4 文書構成

本文書の構成は下記のとおり

- 1 節は、本文書のイントロダクションであり、背景と目的、用語の定義及びここで使われる頭字語リストを含む。
- 2 節は、NIST もしくは NIST が参加するグループが開発した暗号標準やガイドラインに関連する法的命令を示す。
- 3 節は、NIST もしくは NIST が参加するグループが開発した暗号標準やガイドラインに関連する大統領行政府（EOP）からの指令を示す。
- 4 節は、必要な暗号化処理と保護レベルを予め規定した組織特有の方針の概略を示す。
- 5 節は、必要なセキュリティコントロール要件（暗号化要件も含む）を満たすリスク管理方法の概略を示す。
- Appendix A は、参考文献・参照文献のリストである。

2 適用可能な公法

本節は、NIST もしくは NIST が参加するグループが開発した暗号標準やガイドラインに関連する法的命令の要点を示す。

2.1 2002 年電子政府法（FISMA）

Title III of Public Law 107-347 は、2002 年連邦政府情報セキュリティ管理法（the Federal Information Security Management Act of 2002（FISMA））として引用されており、NIST 法（NIST Act）の Section 20 と 21 に組み入れられている。

当該法の第 3543 節は、大統領府に対し、（NIST 法[15 U.S.C. 278g–3] Section 20 に基づく）NIST による標準規格やガイドラインの制定を国家安全保障システムの運用又は実行をコントロールしている他の組織（NSA を含む）と調整するように指示しており、国家安全保障システム向けに開発された標準規格やガイドラインと相補的であることを可能な限り保証することを規定している。

当該法 Section 302 は、商務長官に対し（合衆国法典（U.S.C.）Section 11331 of Title 40 の下で）NIST が制定した標準やガイドラインに準拠した連邦政府情報システムに適合した標準規格やガイドラインを規定するよう指示するものである。Section 302 は、これらの標準規格を、商務長官が連邦政府情報システムの運用効率やセキュリティを向上させるために必要と決めた範囲で強制力があるようにし、また以下の情報セキュリティ標準規格を含まなければならない、と規定している。

(1) NIST 法[15 U.S.C. 278g–3] Section 20(b)に規定されている最低限の情報セキュリティ要件を提供する標準規格

(2) 他の連邦政府情報システムのセキュリティを向上するために不可欠な標準規格

大統領のみがこれらの標準規格を拒否もしくは変更する権限を持つ。

執行機関の長は、商務長官が予め定義した標準よりも厳しい当該機関の監視下にある、情報システムのより費用対効果が高い情報セキュリティの標準を活用することができる。より厳しい標準とは、(1) 少なくとも、商務長官が強制化した適用される標準を含むこと、及び（2）その他の点で、NIST 法[15 U.S.C. 278g–3] Section 20 の定めに従って、NIST から商務長官への標準提案の提出後 6 カ月以内に、商務長官が標準を公布することも要求している Section 3543 of Title 44 U.S.C. Section 302 の下で定められた方針やガイドラインに適合していること、である。

当該法 Section 303 は、NIST 法[15 U.S.C. 278g–3] Section 20 の NIST に対する要求の改定であり、下記を含む：

(1) 情報システムに対する、標準、ガイドライン、関連方式や技術を開発するミッションを負う

(2) 国家安全保障にかかわるシステム（Section 3542(b)(2) of Title 44, United States Code に規定される）以外の情報システムに求められる最低限守るべき要件を含む標準とガイドラインを制定する。国家安全保障にかかわるシステム以外の情報システムとは、（Section 3542(b)(2) of Title 44, United States Code で規定される）国家安全保障システム以外の、機関、機関からの請負業者、又は機関の代理としてのその他の組織からの請負業者が利用又は運用しているシステムのことである

(3) 全機関の運用及び資産に対する適切な情報セキュリティを提供するために最低限守るべき要件を含む標準とガイドラインを制定する。このような標準やガイドラインは、国家安全保障システムには適用しない

Section 303 は、標準とガイドラインが下記項目を含むことを特に求めている：

(1) リスクレベルの範囲に応じて適切なレベルの情報セキュリティを提供する目的に基づき、各機関もしくは各機関の代理機関により収集又は維持される全ての情報と情報システムを分類するために全ての機関が使う標準規格

(2) 各カテゴリに含まれる情報の種類と情報システムを推奨するガイドライン

(3) 各カテゴリにおいて情報と情報システムに求められる最低限守るべき情報セキュリティ要件

(4) 情報セキュリティインシデントの検知と対処に関する定義とガイドライン

実現可能な最大限の範囲で、当該法 Section 303 は NIST に以下を求める：

(1) セキュリティ標準とガイドラインは、特定のハードウェアやソフトウェアを含む特定の製品の使用や調達を要求しないようにすること

(2) そのような標準とガイドラインは、特定された情報セキュリティリスクに対して同等レベルの保護を提供する代替手段を受け入れる十分な柔軟性があること

(3) 商用開発された市販の情報セキュリティ製品が使用可能な、柔軟で性能の優れた標準とガイドラインを使うこと

当該法 Section303 の他の要求事項で、NIST は下記が求められる：

(1) Section 11331 of Title 40, United States Code のもとで発布するために、開発した標準を商務長官に提出する。推奨に加えて、これらの標準は強制力と拘束力があるものになる

(2) 機関に対して、標準とガイドラインへの準拠、情報セキュリティインシデントの検知や取り扱い、情報セキュリティ方針、手順、及び実践に関して、技術的支援を必要に応じて提供する

(3) 情報セキュリティ脆弱性の特徴や影響範囲、及び費用対効果が高い情報セキュリティを提供する手法を見つけ出すために、必要に応じて、調査研究をおこなう

(4) 機関の情報セキュリティ方針や実践のための評価指標や対策を制定し定期的に改定する

(5) 民間の情報セキュリティ方針や実践、及び市販の利用可能な IT 技術の評価を行い、機関が情報セキュリティの強化に活用できるか確認する

(6) 要請に応じて民間を支援し、本節での活動結果を利用し適応する

(7) 国家安全保障システムのために制定されたセキュリティ方針と実践を評価し、機関の情報セキュリティの強化に活用できる可能性があるか評価する

(8) 定期的に本節の下で制定された標準とガイドラインの有効性を評価し、必要に応じて改定する

2.2 経済的及び臨床的健全性のための医療情報技術に関する法律（HITECH）

2009 年経済的及び臨床的健全性のための医療情報技術に関する法律（The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009）は、特定の分野に向けた法律の事例であり、NIST 標準を使用した情報暗号化を規定している。HITECH 法は、2009 年米国復興再投資法（The American Recovery and Reinvestment Act of 2009）の Title XIII として、健康情報技術の採用と有意義な活用を促すことを目的に施行された。HITECH 法の Subtitle D は、健康情報の電子的

伝送に関連するプライバシーとセキュリティに関した内容を取り扱ったものであり、1996 年健康保険ポータビリティ及び説明責任法[1]（Health Insurance Portability and Accountability Act (HIPAA) of 1996）で施行されたルールの市民及び犯罪の観点で補強した規定を一部含んでいる。HITECH 法は、正しく安全性が確保されていない保護対象健康情報（PHI）のセキュリティが破られた際に告知することを義務付けているが、被害を受けた情報が暗号化され読めない状態[2]になっていれば報告義務はないとしている。

2.3 2014 年連邦政府情報システム近代化法

2014 年連邦政府情報システム近代化法（Federal Information Systems Modernization Act of 2014）は、2002 年連邦政府情報セキュリティ管理法（Federal Information Security Management Act of 2002）で義務付けられている行政管理予算局（OMB）の責任の一部を OMB 局長から国土安全保障長官に変更した。第 3553 節は国土安全保障長官に対して次の事項を求めている：

(1) NIST（NIST 法[15 U.S.C. 278g–3] Section 20 の下で）が定めた標準とガイドラインを国家安全保障システムの制御を運用又は実行している機関や組織（NSA を含む）と調整すること。これらの標準とガイドラインを、国家安全保障システムのために制定された標準やガイドラインを補完することを可能な限り保証すること

(2) 政府全体の情報セキュリティ方針とその実践についての作業を調整すること。これには、最高情報責任者協議会（当該法 Section 3603 で規定されている）及び NIST 長官との協議も含む

(3) 国土安全保障省（DHS）が制定した方針、原則、標準及びガイドラインを機関が実施する際に拘束力のある運用指令の実施を展開及び監督すること。並びに、NIST が制定し、商務長官が Title 40 の Section 11331 のもとで発行した適用可能な標準やガイドラインを検討すること

(4) NIST が制定した標準やガイドラインを実施するための DHS が発行する拘束力のある運用指令に関して、NIST 長官と協議すること

(5) 拘束力のある運用指令が Title 40 の Section 11331 のもとで発行する標準やガイドラインと相反しないことを保証すること

また、当該法 3353 節は、Title 40 の Section 11331 のもとで制定し発布する標準やガイドラインについて、国土安全保障長官が商務長官に指示する認可を与えると解釈されるものではないと規定する。さらに、本小節（Title 40 の Section 1131）も、NIST 法[15 U.S.C. 278g–3] Section 20 も、Title 5 も

---

1 https://www.gpo.gov/fdsys/pkg/PLAW-104publ191

2 ただし、データの暗号化は、情報漏えい通知要件を詳しく説明している当座の最終規定に従い、NIST の連邦情報処理標準（FIPS）140-2 に準拠していることを検証しなければならない。また、この HHS ガイダンスは、個人健康記録（PHR）のベンダに適用される当座の情報漏えい通知要件の目的で、識別可能な健康情報を使用したり、読んだり、判読したりできないようにするためにも使用される。その要件は、連邦取引委員会が管理することになっている（次いで、2009 年 4 月 16 日に、PHR による電子健康情報の漏えいに関する消費者への通知についての規制案を発表している）。HHS ガイダンスでは、HITECH 法の目的である情報の保護方法として、破棄する方法と暗号化する方法の 2 つの方法を提示している。破棄は、紙媒体又は電子媒体のいずれかで発見された情報を保護することができる。破棄の方法を満たすためには、紙又はその他のハードコピーメディアは、PHI の読み取り又はその他の方法での再構築ができないように、裁断又は破砕されなければならない。電子メディアは、NIST SP 800-88 に記載されている仕様に従って、消去（クリア）、処分（パージ）、又は破砕されなければならない（74 Fed. Reg. at 19010 参照）。

しくは Title 44 U.S.C に基づく個人のプライバシー保護に関連する情報を含む、認可された情報の使用や開示に関して、大統領、行政管理予算局又はその局長、NIST、もしくは各機関の長官の権限に影響を与えると解釈されるものではないと規定する。

2.4 2014 年サイバーセキュリティ強化法

2014 年サイバーセキュリティ強化法（The Cybersecurity Enhancement Act of 2014）は、NIST のセキュリティ標準化活動を民間への直接サポートも含むように拡張する。セキュリティ標準の責任拡張には暗号標準も含まれる。この拡張は、アメリカ連邦政府以外の組織に関してもサイバーセキュリティへの支援を具体的に認可していることが重要である。

特に、当該法 Title I : サイバーセキュリティに関する公民協調（Sec.101）は NIST 法の改定であり、商務長官が NIST 長官を通して、自発的な合意形成型の産業界主導の標準や手順一式の開発を促進し、支援することを認めている。こうすることによって、高い費用対効果で重要インフラのサイバーリスクを減らすことができる。当該法は NIST 長官に下記の任務を実行するように求める：

(1) 産業界の専門的知識を持った、関連する民間の人材やエンティティ、重要インフラの所有者やオペレータ、セクタ連携協議会、情報共有分析センタ、及びその他関連産業組織と継続的に調整及び連携すること

(2) 国家安全保障の責任を負う機関、特定分野の機関、州や地方政府、他国政府、及び国際機関の長と協議を行うこと

(3) 情報セキュリティへの手段やコントロールを含む、優先順位付けされた、柔軟で繰り返し実行可能で性能が優れていて費用対効果も高い手法であり、重要インフラの所有者やオペレータが自発的に適用してサイバーリスクを特定、評価、管理することを支援する手法を特定すること

(4) 事業上の機密性へのインパクトを軽減し、個人のプライバシーと公民的自由を保護し、自発的な合意形成型の標準と業界ベストプラクティスを取り入れ、国際標準と協調し、かつ法的規制手順の重複を防ぐための手法を含むこと

しかし、当該法は、長官が特定のソリューションを先に指定したり、特定の方法で設計又は製造された製品やサービスを要求することを禁じている。また、サイバーリスク標準を制定する目的で NIST に提供された情報を、連邦、国家、種族、もしくは地方機関が何らかのエンティティの活動を規制するために用いることも禁じている。

当該法の Title II : サイバーセキュリティ研究開発（Sec. 201）は、各機関に対し、サイバーセキュリティの目的に適合するように、既存プログラムを基に、例えば下記の方法を踏まえるように指示している：

(1) 個人のプライバシーを保証し、サードパーティソフトウェアとハードウェアを確認し、内部関係者による脅威に対処する方法

(2) インターネット経由で受け取る情報の源を明確にする方法

(3) クラウド上に保管する情報、又は無線伝送する情報を保護する方法

Title II はまた、各機関が、消費者のプライバシーを守り、デジタルインフラの安全性、信頼性、復元力、及び信用を強化する技術をどのように重視しているかを説明することを要求する。

当該法 Title V：サイバーセキュリティ技術標準の促進（Sec. 502）は、NIST が情報システムセキュリティに関連する国際技術標準を制定する業務に携わっている連邦政府機関と確実に連携することを求めている。また、NIST が適切な民間のステークホルダと確実に協議することを指示している。

当該法 Section 503 は、適切なセキュリティフレームワークとリファレンス材料の開発、及びベストプラクティスの特定を（民間と協議して）サポートする活動が考慮されるように要求している。これは、連邦政府機関がセキュリティとプライバシー要件を定める際に使用するためである。

当該法 Section 504 は、NIST が、ID 管理 R&D 分野において、自発的で費用対効果が高い技術標準、手法、テスト環境、及び規格適合性基準の開発をサポートするプログラムを継続することを求めている。

3 大統領行政府指令

本節は、NIST もしくは NIST が参加するグループが制定した暗号標準やガイドラインに関連する大統領行政府（EOP）の指令を示す。

3.1 国家安全保障大統領指令第 7 号（HSPD-7）：重要インフラの特定、優先順位付け、及び保護

HSPD-7 は、連邦政府の部門や機関が米国の重要インフラ及び重要資源を特定し優先順位を定めて、テロリスト攻撃からそれらを守るための国家方針を構築する。この指令は、商務省に対して、国家安全保障省と連携し、民間、研究機関、学術機関や政府機関と協業してサイバーシステムのための技術を進化させ、重要インフラのその他活動を促進させることを指示している。この中には、国防生産法[3]（Defense Production Act）の定める権限を行使する権利を利用して、産業製品、材料、及びサービスが国家安全保障の要件に則してタイムリーに提供されるよう指示することができる。

3.2 HSPD-12: 連邦政府職員ならびに請負業者の共通 ID 標準指針

この指令は、安全で信頼できる ID 体系に関する連邦政府標準の開発に必須のものである。HSPD-12 は、商務長官に対し、適切な法に則った、安全で信頼できる ID 体系の連邦政府標準を発布することを指示している。その際、国務長官、国防長官、司法長官、国土安全保障長官、行政管理予算局長、及び科学技術政策局長と協議することを指示している。商務長官は、定期的に本標準を見直して、適切に更新を行うことが求められており、その際に関連する機関と協議することが求められている。この指令で目的としている“安全で信頼できる ID 体系”とは、以下を全て満たす ID 体系を意味する：

(a) 職員一人一人の身元を確認できる適切な基準をもとに発行されている

(b) 身元の偽装、改ざん、偽造、テロリストによる不正使用に対し耐性が強い

(c) 速やかな電子的認証が可能である

(d) 公的な認定プロセスを通して認定された信頼できる提供者からのみ発行が可能である

ここで制定する標準は、最低安全レベルから最高安全レベルまで段階的基準を含むように指示されている。これにより、各アプリケーションで適切な安全性レベルを選択できる柔軟性を持たせることができる。

3.3 大統領令第 13636 号：重要インフラのサイバーセキュリティ改善

大統領令第 13636 号 Section 7「重要インフラのサイバーリスクを低減するためのベースラインフレームワーク」では、商務長官が NIST 局長に対して、重要インフラのサイバーリスクを低減するフレームワーク（以下「*サイバーセキュリティフレームワーク*」）の制定を指示することを求めている。その*サイバーセキュリティフレームワーク*の要件は以下のとおりである：

---

[3] https://www.fema.gov/media-library-data/1438002689366c84ffcf6e8476f44e0921a70a4556f88/Defense_Production_Act_2014.pdf

- 方針、事業、技術アプローチに沿ってサイバーリスクに対処する標準、手法、手順、及びプロセス一式を含むこと
- 自発的な合意標準、及び産業界のベストプラクティスをできる限り取り入れること
- 自発的な国際標準が本命令の目的を促進する場合には、当該標準との整合性を図ること
- NIST 修正法（15 U.S.C. 271 et seq）、1995 年国家技術移転促進法（the National Technology Transfer and Advancement Act）（Public Law 104-113）、及び改定 OMB 回覧（Circular）A-119 の要件に沿うこと

*サイバーセキュリティフレームワーク*の要件は以下のとおりである：

- 情報セキュリティの対策と管理を含む、優先順位付けされた、柔軟で再現可能で性能が優れていて費用対効果も高い手法を提供する
- 重要インフラの所有者及び運用者がサイバーリスクを特定、評価、管理することを支援する
- 重要インフラに適用可能な、分野横断のセキュリティ標準やガイドラインの特定に注力する
- 特定のセクタや標準化団体と将来的に連携して改善に取り組むべき分野を特定する
- 技術革新を可能にし、組織間による違いに対する説明責任を負わせるために、技術中立であり、重要インフラセクタがサイバーリスクに対処するよう制定された標準、手法、手順、及びプロセスに適合する製品やサービスを競争市場から選択して利益が得られるようにするためのガイダンスを提示する
- *サイバーセキュリティフレームワーク*を適用する際のエンティティの性能評価を行うためのガイダンスを含む

*サイバーセキュリティフレームワーク*は、事業上の機密性に対する*サイバーセキュリティフレームワーク*及び関連する情報セキュリティ対策又は管理についての影響を特定し軽減するとともに、個人のプライバシーや公民的自由を保護するための手法を含むことも求められる。

*サイバーセキュリティフレームワーク*を制定するにあたり、NIST は公開レビューとパブリックコメントを実施することが求められた。局長はさらに国土安全保障長官、国家安全保障局、特定分野の機関や行政管理予算局（OMB）を含む他の関連する機関、重要インフラの所有者やオペレータ、及びその他の関係者と協議することも求められている。

3.4 OMB 回覧 A-119：自発的な合意標準の制定と利用及び適合性評価活動への連邦政府の参加

OMB 回覧（Circular）A-119 は、自発的な合意標準の連邦政府の利用と制定、及び適合性評価活動に関する方針を定めている。1995 年国家技術移転促進法（Public Law 104-113）は、A-119 にあった既存方針を成文化して報告要件を規定するとともに、NIST が政府機関の適合性評価活動を調整することを認めたものである。行政管理予算局（OMB）は、以下の目的のため当該回覧の改訂版を発行した：

- 1995 年国家技術移転促進法と整合が取れるように回覧で使用する用語を定める
- OMB への報告書作成に関するガイダンスを各機関に発行する
- 商務長官が適合性評価に関するポリシーガイダンスを発行するように指示する
- 変更点を明確化する

3.5 OMB 回覧（Circular）A-130：戦略資源としての情報管理

行政管理予算局（OMB）回覧（Circular）A-130[4]は、連邦政府の情報、人事、機器、資金、IT リソース及びインフラやサービスの支援に関する計画、予算、ガバナンス、取得及び管理のための全般的な方針を示している。本回覧の附則では、連邦政府が保有する情報リソースの保護と個人識別情報（PII）の管理に関する責任についても含んでいる。本回覧の要求事項は、連邦政府行政部門の全ての機関の情報リソース管理活動に適用される。回覧 A-130 の要求事項は、紙や電子情報も含む全てのメディア（除外注釈がない限り）に記録されている全ての情報リソースに関する管理活動に適用される。ある機関がサービス提供者となる場合でも、適用可能な本回覧で求められる要求事項への準拠に関する最終的な責任は（サービス提供者に）移管されない。各機関は、サービス提供者との間の関連する契約書にそのサービス提供者が負う責任範囲を記すことが求められる。各機関は、国家安全保障システム（44 U.S.C § 3552[5]で定義されている）に対して本回覧を適用する必要はないが、適切な場合には適用することを推奨する。国家安全保障システムに関しては、各機関は適切な法令、大統領令、指令及び機関内部の方針に従わなければならない。

他の多くのサイバーセキュリティ関連指令や命令と異なり、回覧 A-130 は暗号化やデジタル署名に対する特定の要求事項を強制している。以下の資料は、暗号化及び背景にあるリスク管理規定にかかわる特に目立つ要求事項を特定している。以下の各小節では、参照しやすくするために、リストに関連する節番号は当該回覧で使っているのと同じ番号を付けている。

3.5.1 プライバシー及び情報セキュリティ条項

Section 5, “Policy,” subparagraph f, “Privacy and Information Security,” subparagraph 2), “Information Security,”では、各機関に対して、下記のように適切な予防策を施すように求めている：

a) CIO が、当該機関の上級情報セキュリティ責任者を任命し、機関内全体の情報セキュリティプログラムを 2014 年連邦政府情報セキュリティ近代化法に沿う形で制定させ、維持させることを確認する

b) 情報への認可されていないアクセス、不正使用、不正開示、障害、改ざん、又は破棄の結果を招くリスクに見合った方法で情報を保護する

c) 行政管理予算局（OMB）から発行されているセキュリティ方針を実装し、同時に商務省、国土安全保障省（DHS）、共通役務庁（GSA）及び人事管理局（OPM）が発行する要求事項にも対応する。これには、NIST FIPS、NIST SP（例：800 シリーズガイドライン）、OMB からの割当や指令、NIST 機関内部報告書[6]（NISTIR）に記されている標準とガイドラインに対応することも含まれる

---

4 この回覧は、プライバシー、機密性、情報の質、普及、統計政策など、情報資源管理に関する多くの具体的な問題に触れているが、これらのトピックは、OMB ウェブサイトに掲載されている他の行政管理予算局（OMB）の方針でより詳しく説明されている。各機関は、この回覧に記載されている方針と、他の OMB 方針ガイダンスに記載されている方針を、相互に整合性のある方法で実施しなければならない。

5 https://www.gpo.gov/fdsys/pkg/USCODE-2014-title44/html/USCODE-2014-title44-chap35-subchapIIsec3552.htm

6 NISTIR は、専門家向けに関心のある技術的特性の研究内容を記述したものである。NIST のサイバーセキュリティの NISTIR は、以下のサイトで入手可能。http://csrc.nist.gov/publications/PubsNISTIRs.html.

3.5.2 電子署名条項

Section 5, “Policy,” subparagraph g, “Electronic Signatures,” subparagraph 3), “Information Security,”は、各機関が下記を満たすことを求める：

1) 機関とやり取りをする個人もしくはエンティティが、電子的に情報を提出又は機関と取引することが可能であって、機関が電子的記録を保持することが可能な場合には、その選択を認める。電子的記録とそれに関連する電子署名は、電子形態であるというだけの理由のために、法的にその効果、有効性、又は執行可能性が否定されてはならない

2) 民間商取引での電子的な契約形態、署名及び記録保管の利用を、以下の形態間での法的等価性を保証することにより推進する。: 書面契約と電子形態契約、自署署名と電子署名、及び他の法的要件による書面（専門用語でいうところの“記録”）と同じ情報の電子形態

3) 職員と請負業者が電子署名の一形態であるデジタル署名を使うことを支援する手順を開発し実践する

3.5.3 政府全体としての責任

以下の条項が、Section 6, “Government-wide Responsibilities.”で決められている。

a. 商務省

商務長官は以下を実行しなければならない：

1) 連邦政府情報システム、及び連邦政府に代わって情報を生成、収集、処理、保管、伝送、公布、又は破棄するシステムにおける情報のセキュリティとプライバシーに関する標準とガイドラインを開発し発行する [7]。

2) IT の開発と利用に関連して科学技術に関する助言サービスを行政管理予算局（OMB）及びその他の機関に提供する [8]

3) 電気通信技術、及び連邦電気通信システムの改善、拡張、試験、運用及び使用に関する調査と評価を実施し、行政管理予算局長及びその他適切な機関に、それら調査の結果から得られる推奨事項を助言する

4) 国務長官及び行政管理予算局長と協議のうえ、連邦政府情報活動に影響を与える国際電気通信での課題に関する計画、方針、及びプログラムを開発する

5) 電気通信及び情報処理技術における標準化のニーズを特定し、国防総省及び共通役務庁（GSA）と協議して、そのような技術の効果的な適用を担保する標準を開発する [9]。

6) 連邦政府が（国務長官と協議のうえ）国内ならびに国際の IT 標準を定める代表となっていることを保証し、そのような活動について行政管理予算局長に助言する [10]

---

[7] NIST 法（15 U.S.C. § 278g-3）

[8] NIST 法（15 U.S.C. § 278g-3）に基づく。

[9] NIST 法（15 U.S.C. §§ 272(b), 278g-3）及び OMB A-119（自発的な合意標準の制定と利用及び適合性評価活動への連邦政府の参加）に基づく。

[10] NIST 法（15 U.S.C. §§ 272(b), 278g-3）及び OMB A-119（自発的な合意標準の制定と利用及び適合性評価活動への連邦政府の参加）に基づく。

7) 国防総省（DOD）及び国土安全保障省（DHS）の技術支援を受け、新しい情報技術を評価し、セキュリティ脆弱性を評価する

9) サイバーセキュリティフレームワークの開発を主導し、大統領令第 13636 号「重要インフラのサイバーセキュリティ改善」に従った重要インフラのサイバーリスクを低減する

3.5.4 連邦政府情報資源の保護及び管理のための一般要件

Section 3, “General Requirements” の下にある Appendix I, “Responsibilities for Protecting and Managing Federal Information Resources”は、以下を指示している：

a. 各機関は、その機関内全体のリスク管理プロセスを実装しなければならない。そのプロセスとは、3 つの組織的段階（すなわち、組織レベル、ミッションもしくはビジネスプロセスレベル、及び情報システムレベル）にわたって継続的に情報セキュリティとプライバシーのリスクを定義、評価、対処、及び監視することである [11]。

b. [適用外のため、本稿から削除。]

c. 個人識別情報（PII）を共有する機関は、適宜、PII を共有している他の機関やエンティティに対して、PII を共有する機関が決めた NIST FIPS Publication 199 での特定の機密性インパクトレベルに準拠した情報システムで PII を維持管理することを求めなければならない。

d. PII を他の機関もしくはエンティティと共有している機関は、必要に応じて、契約書やデータ利用合意、情報交換合意、覚書などの合意書面により、条件（特定のセキュリティとプライバシー制御の選定や実装など）を強制しなければならない。この条件により、PII の生成、収集、使用、処理、保管、維持、配布、開示、及び破棄を管理する。

e. 各機関は、管理された非機密情報（CUI）を保護しなければならず、NIST FIPS 及び NIST（800 シリーズ）SP[12]を適切に適用しなければならない。これには、独占情報の開示を法的に認可された場合に制限することや、適切な利用条件を強制することで、継続的に情報の機密性を維持することを確認する義務を負わせることが含まれる。

f. 各機関は、全ての適用される法令、規制、及び方針の要求事項を遵守し、効率的な情報セキュリティ及びプライバシープログラムを作成して維持しなければならない。この中には、プライバシーインパクト評価やプライバシーリスクを管理する様々なツールを利用することも含まれる。

g. 各機関は、行政管理予算局（OMB）が発行する方針、及び商務省、国土安全保障省（DHS）、共通役務庁（GSA）、及び人事管理局（OPM）が発行する要求事項も実装しなければならない。この中には、NIST FIPS、NIST（800 シリーズ）SP、及び必要に応じて OMB からの指令、NISTIR に記されている標準とガイドラインに対応することも含まれる。

3.5.5 連邦政府情報リソースの保護及び管理のための具体的要件

Section 4, “Specific Requirements”の下にある Appendix I, “Responsibilities for Protecting and Managing Federal Information Resources”は、以下を指示している：

---

[11] NIST SP 800-39 “*情報セキュリティリスク管理：組織、ミッション、及び情報システムの視点*” では、リスク管理のプロセス及び戦略に関する追加情報を提供している。

[12] NIST FIPS 及び SP 800 シリーズの出版物は、それぞれ以下のサイトで入手可能。 http://csrc.nist.gov/publications/PubsFIPS.html 及び http://csrc.nist.gov/publications/PubsSPs.html

a. セキュリティ分類

各機関は、以下を行わなければならない：

1) NIST SP 800-18 及び SP 800-37 に従って、情報システムの認可境界を規定する。

2) 情報及び情報システムを、FIPS 199 及び NIST SP 800-60 に従って分類する。その際、組織運営及び資産、個人、他組織、及び国家への潜在的に起こり得るセキュリティ及びプライバシーに関する被害のインパクトを考慮する。

c. 計画、管理及び評価

各機関は、以下を行わなければならない：

5) 情報システム及びそのシステムの運用環境[13]に対するセキュリティコントロールを選択・実装するためのプロセスを採用する。そのプロセスは、FIPS 200 での最低限守るべき情報セキュリティ要求事項、及び NIST SP 800-53 のセキュリティコントロールのベースラインを基に適切に調整した内容を満たす。

6) 情報システム及びプログラムに対するプライバシーコントロールを選択・実装するためのプロセスを採用する。そのプロセスは、OMB ガイダンスに記載された適用可能なプライバシー要求事項を満たす。OMB ガイダンスには、本回覧の Appendix I や OMB 回覧 A-108、プライバシー法の下におけるレビュー、報告、公表に関する連邦政府機関の責任を含むが、それらに限られるものではない。

7) 適切なシステムセキュリティエンジニアリング基本指針、コンセプト、手法、実践及び技術を使って情報システムセキュリティを実装する。

8) FIPS 200 の最低限守るべき情報セキュリティ要求事項、及び NIST SP 800-53 のセキュリティコントロールのベースラインを基に適切に調整した[14]内容を満たすようなセキュリティコントロールの選択方法及び実装方法について文書化した情報システムのセキュリティ計画を開発し維持する。

10) 連邦政府職員及び請負業者に対し、多要素認証、デジタル署名、及び ID 保証を提供し、政府機関間で相互に利用可能であり全ての行政府機関で受け入れられる暗号化機能を提供する効果的なセキュリティコントロールを導入する。

11) 連邦政府機関の施設にアクセスする際に職員及び請負業者が使用する ID 資格証の開発及び利用[15]に関する政府機関全体の要求事項を遵守する。

12) 共通のコントロールを指定することで、複数の機関の情報システム又はプログラムに継承できる費用対効果の高いセキュリティとプライバシー機能[16]を提供する。

---

[13] 運用環境には、情報システムが情報を処理し、保存し、送信する物理的な環境が含まれる。機関は、セキュリティ対策を選択、実施、文書化及び評価をする際に、環境を考慮すべきである。

[14] 機関は、OMB 方針に則して調整活動を実施しなければならない。

[15] NIST SP 800-116, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*は、物理的アクセス制御システムにおける政府全体の標準 ID 資格証である PIV 資格証の使用に関する追加情報を提供している。物理的アクセス制御システムは情報システムとみなされ、それには共有又は分離されたネットワーク内のサーバ、データベース、ワークステーション、及びネットワーク設備などが含まれる。

[16] 共通のコントロールでインパクトレベルの異なる複数の機関の情報システムを保護する場合、そのコントロールは、情報システムの中で最もインパクトレベルの高いレベルで実施しなければならない。その

13) セキュリティとプライバシーコントロールが正しく実装されているか、想定通りに運用されているか、適用可能な要求事項への適合性の確認及びセキュリティとプライバシーリスクへの管理が十分であるかといった観点で、選択され実装された全てのセキュリティとプライバシーコントロールの評価を実施し文書化する。

14) セキュリティとプライバシーコントロールの評価を、情報システムの運用開始前に、またそれ以降定期的に実施し文書化する。定期評価は、その機関の情報セキュリティ継続モニタリング（ISCM）、及びプライバシー継続モニタリング（PCM）戦略ならびにその機関のリスク許容度に則して定める頻度で行う。

i. 連邦政府情報及び情報システムの保護を強化するための具体的保護対策 [17]

各機関は、以下を行わなければならない：

4) 機微性又は重要性の高い情報資源（例：情報システム、システムコンポーネント、アプリケーション、データベース、情報など）を、それらの資源の機微度又は重要度に基づいて適切な保護レベルを持つ別個のセキュリティドメインに分離する。

8) サポートされていない情報システム及びシステムコンポーネントの使用を禁止し、適切な保護や安全性が確保できないシステム及びコンポーネントは高い優先度で更新又は交換[18]を確実に行う。

11) 政府機関全体の ID 管理標準[19]に則し、職員と請負業者に多要素認証の利用を要求する。

12) 職員と請負業者のためにデジタル署名の利用を支援するプロセスを開発し実施する。

ようなコントロールを情報システムの中で最もインパクトレベルの高いレベルで実施できない場合、機関はこの状況をリスク評価に織り込み、適切なリスク緩和措置（セキュリティコントロールの追加、セキュリティコントロールパラメータの割り当て値の変更、代替コントロールの実施、ミッション又は事業プロセスのある側面での変更、又はよりインパクトレベルが高いシステムについて適切なレベルの保護が可能な独自のドメインへの分離、など）を取らなければならない。

[17] NIST SP 800-53“*連邦政府情報システム及び連邦組織のためのセキュリティコントロール及びプライバシーコントロール*”には、追加のセキュリティ保護対策に関する情報が記載されている。

[18] ソフトウェアパッチ、ファームウェアアップデート、部品交換、保守契約などの利用により、開発者、ベンダ、又は製造事業者がサポートしなくなったハードウェア、ソフトウェア、ファームウェアコンポーネントを含む。NIST SP 800-53“*連邦政府情報システム及び連邦組織のためのセキュリティコントロール及びプライバシーコントロール*”には、サポートされていないソフトウェアコンポーネントに関する追加のガイダンスが記載されている。

[19] 国土安全保障大統領指令 12“*連邦政府職員ならびに請負業者の共通 ID 標準指針*”に従い、NIST FIPS 201 は、スマートカードの形式要素（PIV カード）として職員及び請負業者のための初期の政府全体の ID 管理標準を記述している。新世代コンピュータデバイス、特にモバイル端末の出現に伴い、PIV カードの使用は技術的に進化し、NIST SP 800-157 で規定されているように、モバイル端末に直接配備できる他の形式要素を含むようになった。この代替手段に関連する PIV 資格証は、派生 PIV 資格証と呼ばれる。派生 PIV 資格証は、NIST SP 800-63 の派生資格証の一般概念に基づいている。派生 PIV 資格証を PIV カード保持者に発行する際に、ID 証明及び身元調査処理を繰り返すことを要求しない。ユーザは、派生 PIV 資格証を受け取るために、有効な PIV カードの所有及び管理を証明するだけである。

13) 機関が使用し、連邦 PKI 方針に従って発行した全ての公開鍵基盤（PKI）証明書が、使用者の署名、暗号化目的、認証及び認可に使用される際に、連邦 PKI トラストアンカー[20]の有効性を確認する。

14) FIPS 199 で中インパクト又は高インパクトに分類される全ての情報を保管時及び伝送時に暗号化する [21]。例外として、それらの情報を暗号化することが技術的に不可能な場合、もしくはその機関それぞれのミッション、機能、又は運用を実行する能力に明らかに影響を与える場合であって、暗号化しないことのリスクを認可権限がある責任者が許容し、当該機関の CIO が、（必要に応じて）上級プライバシー責任者（SAOP）の助言のもと、承認した場合にはこの限りではない。

15) NIST 標準とガイドラインに従った暗号化アルゴリズム及び認証済暗号化モジュールを導入する。

16) 合法的にアクセスする必要がある個人もしくは個人の代わりに実行されるプロセスのみに、機微情報の復号ができる権限を持たせることを確実にする。

17) 連邦政府情報の安全性とアクセスを確実にするため、データレベルの保護とアクセスコントロールを実施する。

18) ドメインネームシステム（DNS）で識別される全ての連邦政府システム及びサービスがドメインネームシステムセキュリティ（DNSSEC）により保護されており、全てのシステムが DNSSEC で保護された情報を検証することができることを確実にする [22]。

m. 暗号化

リスク評価の結果、必要性が指摘された場合、その機関は、ネットワーク、システム、アプリケーション及びデータを含む複数のレイヤーで実装された物理的かつ論理的な代替防御策で保護されていない限り、保管及び伝送している連邦政府情報を暗号化しなければならない。保管及び伝送している情報を暗号化することで、当該情報の機密性と完全性を保護することにつながり、認可されていない開示もしくは改ざんを受けにくくする。各機関は、FIPS 199 に従って中インパクト又は高インパクトに分類された連邦政府情報に対して、暗号化要件を適用しなければならない。例外として、それらの情報を暗号化することが技術的に不可能な場合、もしくはその機関それぞれのミッション、機能、又は運用を実行する能力に明らかな影響を与える場合にはこの限りではない。暗号化の利用が技術的に不可能な場合、例えば老朽化したレガシーシステムなどの場合、その機関は、保護技術を導入することができる最速のタイミングで適切なシステムやシステムコンポーネントへの更新又は交換を行わなければならない。必要な暗号技術を使用しないで情報システムを運用することを選択した責任者が認可を得るためには、そうすることによるリスクを注意深く評価しなければならず、かつ（必要に応じて）上級プライバシー責任者（SAOP）と協議の上、当該機関の CIO による例外認可を書面で受けなけ

---

[20] トラストアンカーは、連邦 PKI 管理局が運営する連邦 PKI ルート証明書のことを指す。このルート証明書は、全ての連邦 PKI 証明書の信頼の源である。更なる情報は、https://www.idmanagement.gov 及び連邦 PKI 方針を参照されたい。

[21] 組織の情報がネットワーク上を移動しているときや、ストレージデバイスに保存されているときに暗号化することで、当該情報が継続的に保護されていることが保証され、徹底したセキュリティ戦略による防御を推進させる。

[22] DNSSEC は、インターネット基盤の重要なコンポーネントである。DNSSEC により、クライアントは、変換を行う権限を持つサーバから全ての変換が提供されていること、及びサーバからの変換応答がクライアントに到達する前に改ざんされていないことを、暗号学的に検証できる。

ればならない。本方針で取り扱っている連邦政府情報システムに使用する暗号技術として、FIPS 承認暗号のみが承認されている。

n. デジタル署名

デジタル署名は、認証や否認防止機能を提供し、情報が日々扱われているか将来の利用のためにアーカイブされているかに関わらず、連邦政府情報の完全性を保証することで、様々なセキュリティ脆弱性を緩和することができる。さらに、デジタル署名は、各機関がミッションやビジネスプロセスを効率化し、マニュアル処理からより自動的な処理、例えばオンライン処理などに移行する助けとなる。この技術が提供する利点のため、行政管理予算局（OMB）は各機関が連邦 PKI 方針及び NIST 標準とガイドラインに沿ったデジタル署名機能を実装することを期待している。各機関は、その職員と請負業者に対して、個人 ID 認証（PIV）資格証のデジタル署名機能を使うことを要求しなければならない。PIV 適用の範囲から外れる個人に対して、各機関は、デジタル署名を使う時には承認された連邦 PKI 資格証を活用すべきである。

3.5.6 回覧 A-130 で引用されている NIST ドキュメント

回覧（Circular）A-130 では、下記の NIST 文書が参考資料として引用されている：

8) National Institute of Standards and Technology Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems.

9) National Institute of Standards and Technology Federal Information Processing Standards Publication 200, Minimum Security Requirements for Federal Information and Information Systems.

10) National Institute of Standards and Technology Federal Information Processing Standards Publication 201, Personal Identity Verification of Federal Employees and Contractors.

11) National Institute of Standards and Technology Special Publication 800-18, Guide for Developing Security Plans for Federal Information Systems.

12) National Institute of Standards and Technology Special Publication 800-30, Guide for Conducting Risk Assessments.

13) National Institute of Standards and Technology Special Publication 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.

14) National Institute of Standards and Technology Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System View.

15) National Institute of Standards and Technology Special Publication 800-47, Security Guide for Interconnecting Information Technology Systems.

16) National Institute of Standards and Technology Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.

17) National Institute of Standards and Technology Special Publication 800-53A, Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans.

18) National Institute of Standards and Technology Special Publication 800-59, Guideline for Identifying an Information System as a National Security System.

19) National Institute of Standards and Technology Special Publication 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories.

20) National Institute of Standards and Technology Special Publication 800-63, Electronic Authentication Guideline.

21) National Institute of Standards and Technology Special Publication 800-73, Interfaces for Personal Identity Verification.

22) National Institute of Standards and Technology Special Publication 800-76, Biometric Specifications for Personal Identity Verification.

23) National Institute of Standards and Technology Special Publication 800-78, Cryptographic Algorithms and Key Sizes for Personal Identity Verification.

24) National Institute of Standards and Technology Special Publication 800-79, Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI).

25) National Institute of Standards and Technology Special Publication 800-116, Guidelines for the Use of PIV Credentials in Physical Access Control Systems (PACS).

26) National Institute of Standards and Technology Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).

27) National Institute of Standards and Technology Special Publication 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations.

28) National Institute of Standards and Technology Special Publication 800-157, Guidelines for Derived Personal Identity Verification Credentials.

29) National Institute of Standards and Technology Special Publication 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations.

30) National Institute of Standards and Technology Special Publication 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations.

31) National Institute of Standards and Technology Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.

32) National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity.

33) National Institute of Standards and Technology Supplemental Guidance on Ongoing Authorization: Transitioning to Near Real-Time Risk Management.

3.6 OMB 通知文書（Memorandum）M-06-16：組織の機微情報保護

OMB 通知文書 M-06-16 は、NIST が遠隔での情報を保護するためのチェックリストを提供していると記している。チェックリストを提供する意図は、情報が機関所在地の外部から消去されたりアクセスされたりする際の物理的セキュリティコントロールの不足を補うためである。NIST チェックリストの利用に加えて、OMB M-06-16 は、副長官もしくは副長官に書面で指名された者が書面にて“機微ではない（non-sensitive）”と決定したデータを除いて、全ての省庁及び政府機関は当該機関の情報を持ち出すモバイルコンピュータ／デバイス上の全情報を暗号化することを推奨している。また、リモートアクセスは、二要素認証でのみ許可し、そのうちの一要素がアクセスするコンピュータとは別のデバイスによって提供されている場合に限ることを推奨している。

3.7 OMB 通知文書 M-06-18：HSPD-12 実装のための製品とサービスの入手

OMB 通知文書 M-06-18 は、国土安全保障大統領指令-12（HSPD-12）“*連邦政府の職員と請負業者のための共通 ID 標準に関する方針*”の実施のための製品及びサービスの取得についての更新指令を提供し、また実施作業の状況も示している。

HSPD-12 は、HSPD-12 を実装するのに必要となる特定の製品やサービスを試験及び評価するための評価プログラムを NIST と共通役務庁（GSA）が構築したことを記している。また、NIST が NIST 個人 ID 認証プログラム（NPIVP）を構築し、連邦情報処理標準（FIPS 201）で求めている個人 ID 認証（PIV）のコンポーネントやサブシステムを試験して認証すると記している。本通知文書が署名された時点で、NPIVP 認証プログラムが提供された。このプログラムでは、PIV カードアプリケーションと PIV ミドルウェアが FIPS 201 及び NIST SP 800-73 “*個人 ID 認証インタフェース仕様*”に適合していることを試験して認証する。また、NIST は、NIST SP 800-85A “PIV カードアプリケーション及びミドルウェア試験ガイドライン”において派生試験要件を公開したことも提示している。NPIVP プログラムの全ての試験が、現在、暫定の NPIVP 試験施設として指定されている第三者試験ラボにて実施されている。

FIPS 140-2 “*暗号モジュールセキュリティ要件*”[23]は、PIV カード及び暗号機能を実行するその他の製品の暗号モジュールに対して試験及び認証を行うことを要求する。この試験は、NPIVP 試験を実施する指定を受けた第三者認定施設にて実施される。

3.8 OMB 通知文書 M-07-16：個人識別情報漏えいに対する防止策及び対応

OMB 通知文書 M-07-16 は、OMB 通知文書にサインされてから 120 日以内に、情報漏えい[24]の際の通知方針の制定と実施を全ての機関に求めている。本通知文書は、暗号化、強力な認証処理、及びその他のセキュリティコントロールを使用して、情報が非認可者によって使用されないようにすることを特に推奨している。本通知文書の付録には、情報を保護するために適切な保護措置が講じられていることを保証する一方、機関が情報漏えいの際の通知方針を策定しなければならないフレームワークの概要を記載している。そのフレームワークの要素として、以下の要求事項が含まれている：

a. 全ての情報及び情報システムへのインパクトレベルの割当。各機関は、FIPS 199 “*連邦政府情報及び情報システムのセキュリティ分類標準*”に概要が示されたプロセスに則って、全ての情報と情報システムを標準が示す 3 つのインパクトレベル（すなわち、低、中、高）に分類しなければならない。各機関は、一般に、機微な個人識別情報（及びそのような情報を扱う情報システム）を中もしくは高インパクトに分類するようにすべきである。

b. 最低限のセキュリティ要求事項及びコントロールの実施。上記で規定したインパクトレベルごとに、各機関は最低限のセキュリティ要求事項及び最低限（ベースライン）のセキュリティコントロールを実施しなければならない。それらの内容は、FIPS 200 “連邦政府情報及び情報シ

---

[23] 暗号モジュール認証プログラムによる FIPS 140-2 の実施は、FIPS PUB 140-2 及び暗号モジュール認証プログラムの実施ガイダンスに従って行われることに注意されたい。このガイダンスは、FIPS 140-2 に関連する追加の説明／ガイダンスを掲載するために定期的に更新される。

[24] 本方針において、“漏えい”という用語は、コントロールの喪失、危殆化、不正な開示、不正な取得、不正なアクセス、又はこれらに類する用語で、認可ユーザ以外の者が、又は認可されていない目的のために、物理的又は電子的に個人を識別できる情報にアクセスする、又はアクセスできる可能性がある状況を指すものなどを包含して使用される。

ステムに対する最低限順守すべきセキュリティ要求事項”及び NIST SP 800-53“連邦政府情報システムのための推奨セキュリティコントロール”[25]にそれぞれ定められている。

c. 情報システムの認証及び認定。各機関は、当該機関の運用と資産を支援する全ての情報システムを認証し認定（C&A）しなければならない。これには、他の機関、請負業者もしくは他のソースが提供又は管理しているシステムも含まなければならない。C&A を実施するための具体的な手法は NIST SP 800-37“*連邦政府情報システムのセキュリティ認証及び認定ガイド*”[26]に示されており、これには一定レベルのセキュリティコントロールを継続的に監視するためのガイダンスも含まれている。各機関の継続監視では、情報の保護のために使っている管理、運用、及び技術的コントロールの一部分について評価（例：プライバシーインパクト評価）を行うべきである。

本通知文書の要求事項には以下も含まれる。1）副長官[27]もしくは副長官に書面で指名された上級レベルの者が書面にて“機微ではない”と決定したデータを除いて、組織の情報を持ち出すモバイルコンピュータ／デバイス上の全情報に対して、NIST 認証暗号モジュール[28]を使って暗号化すること、2）リモートアクセスは、二要素認証でのみ許可し、そのうちの一要素がアクセスするコンピュータとは別のデバイスによって提供されている場合に限ること。

3.9 OMB 通知文書 M-08-23：連邦政府ドメインネームシステム（DNS）基盤の安全性確保

OMB 通知文書 M-08-23 は、連邦政府に対して、2009 年 1 月までに最上位.gov ドメインではドメインネームシステムセキュリティ拡張（DNSSEC）を用いるよう要求した。最上位.gov ドメインには、レジストラ、レジストリ、及び DNS サーバ処理を含む。この方針は、最上位.gov ドメインは DNSSEC 署名され、安全に委任されたサブドメインが利用できるプロセスを構築することを求めている。最上位.gov ドメインに署名することは、DNSSEC の幅広い展開のために欠くことのできない重要な処理で、DNSSEC の利便性を高め、各機関による下位レベルでの展開を簡単にする。

本通知文書は、さらに DNSSEC が適用可能な情報システム全てに対して DNSSEC を展開するための行動計画とマイルストーンを作成することも各機関に求めた。適切な DNSSEC の機能を、2009 年 12 月までに展開し、運用開始することを求めた。この計画では、NIST SP 800-81“*安全なドメインネームシステム（DNS）展開ガイド*”の要求事項に従い、また NIST SP 800-53r1[29]“連邦政府情報システムのための推奨セキュリティコントロール”に記されている特有の要求事項に対処することになっていた。この計画はまた、NIST SP 800-53r1 にて求められている当時の DNSSEC 要求事項への各機関の現状の順守レベルを報告し、DNSSEC 署名ゾーンを運用するための要求事項の範囲を想定した行動計画及びマイルストーンを文書化することにもなっていた。SP 800-53 のコントロール SC-20 は、

---

[25] 現在の SP 800-53 4 版のタイトルは“連邦政府情報システム及び連邦組織のためのセキュリティコントロールとプライバシーコントロール”である。

[26] SP 800-37 Revision 1“*連邦政府情報システムのリスク管理フレームワークの適用ガイド：セキュリティライフサイクルアプローチ*”として再発行された。なお、認証はもはや必要なく、C&A という用語も廃止されたことに留意されたい。

[27] 行政府以外の機関は、副長官に相当する人に相談すべきである。

[28] 認証済み暗号モジュールについての説明は、NIST ウェブサイト http://csrc.nist.gov/cryptval/を参照されたい。

[29] この通知文書は、以前のバージョンである Revision 1 を参照している。この出版物は更新されている。現在の改訂版は Revision 4 である。

FISMA 情報システム全て（低インパクトのシステムも含め）に対象を拡張することが Revision 3 で求められた。この計画では、全ての機関の.gov ドメインが 2009 年 12 月までに DNSSEC 署名が確実に行われることになっていた。

3.10　OMB 通知文書 M-11-33：2011 年連邦政府情報セキュリティ管理法及び機関によるプライバシー管理に関する報告指示

OMB 通知文書 M-11-33 には、連邦政府情報セキュリティ管理法及び機関によるプライバシー管理に関する報告についてのよくある質問（FAQ）が含まれている。本通知文書に記載されている以下のよくある質問は暗号アプリケーションに関係するものである：

国防総省（DOD）及び国家情報長官官房（ODNI）も行政管理予算局（OMB）方針及び NIST ガイドラインに従わなければならないのか？

はい。国家安全保障に関わらないシステムの場合、DOD 及び ODNI においても OMB 方針及び NIST ガイドラインを内部方針に反映することになっている。

国家安全保障システムに関しては、Joint Task Force Transformation Initiative (JTFTI) Interagency Working Group が、民間、防衛及びインテリジェンスコミュニティ（IC）からの代表メンバーとともに、2009 年開始時から活動を継続して、連邦政府内の共通情報セキュリティフレームワークを構築している。この活動を通して、DOD、ODNI 及び NIST は共同で以下の出版物を発行してきた：

- NIST SP 800-37, Revision 1, *リスク管理フレームワークを連邦政府情報システムに適用するためのガイド*、2010 年 2 月発行
- NIST SP 800-38A, *ブロック暗号利用モードにおける推奨事項*、2001 年 12 月発行
- NIST SP 800-39, *情報セキュリティリスク管理：組織、ミッション、及び情報システムの視点*、2011 年 3 月発行
- NIST SP 800-53 Revision 3[30], *連邦政府情報システム及び組織のための推奨セキュリティコントロール*、2009 年 8 月発行

これらのガイドラインは共同で発行されたものなので、国家安全保障システムにおける DOD 及び ODNI の方針はこれらのガイドラインを反映すべきである。

NIST の出版物の使用が求められるか？

はい。国家安全保障関係以外のプログラム及び情報システムでは、各機関は、行政管理予算局（OMB）から除外の指定を受けていない限り、NIST 標準及びガイドラインに従わなければならない。既存の情報システムに関しては、各機関は、OMB から異なる指示を得ていない限り、NIST 標準及びガイドラインの発行日から 1 年以内にそれらに準拠することが期待される。NIST 出版物の改訂版に対する 1 年以内での準拠という期限は、当該出版物の中の新規や更新部分に関してのみ適用される。開発中の情報システム又は大幅な変更を進めている途中の既存システムについ

[30] この通知文書は、以前のバージョンである Revision 3 を参照している。この出版物は更新されている。現在の改訂版は Revision 4 である。

て、各機関には、当該情報システムが展開される時点で、即座に NIST 出版物に準拠していることが期待される。

NIST ガイドラインには柔軟性があるか？

はい。各機関は、行政管理予算局（OMB）方針に即して NIST 標準及びガイドラインに従うことが求められているが、NIST ガイドライン（特に SP-800 シリーズの）には、各機関がどのように適用するかといった点で柔軟性がある。しかしながら、NIST 連邦情報処理標準（FIPS）出版物への準拠は必須である。OMB が追加の実施方針を指定している場合を除いて、NIST ガイドラインは一般的に各機関にそれぞれのアプリケーションでの自由裁量を認めている。従って、各機関による NIST ガイドライン適用の結果、異なるセキュリティソリューションになる可能性があるが、それらは同じように容認でき、ガイドラインに準拠している。

FISMA、行政管理予算局（OMB）方針及び NIST 標準とガイドラインは、各機関のセキュリティプログラムがリスクベースであることを求めている。許容可能なリスクレベルを決定する責任者は誰か（例：CIO、プログラム実行責任者、システム所有者、もしくは IG)？IG による独立評価もまたリスクベースなのか？彼らが合意しない場合はどうなるのか？

各機関の長は、最終的に当該機関が許容できるリスクレベルを決定する責任を負う。システム所有者、プログラム実行責任者及び CIO はその決定を行うための情報を提供する。このような決定は、OMB 方針、及び NIST 標準とガイドライン（特に FIPS 199 "*連邦政府情報及び情報システムのセキュリティ分類標準*"、FIPS 200 "*連邦政府情報及び情報システムに対する最低限順守すべきセキュリティ要求事項*"、及び SP 800-39 "*情報セキュリティリスク管理*"）を反映していなければならない。情報システムの認可責任者は、あらゆる残余リスクを許容することに対する責任があり、つまり当該システムのセキュリティを管理する責任を負っている。

IG 評価は、各機関がリスクベース手法を当該機関のミッションや事業機能の実行を支援する情報セキュリティプログラムや情報システムに適用していることを、独立して評価することを意図している。例えば、個々のセキュリティ認可の保証として評価をレビューする場合、IG は通常以下の観点で評価する：1）評価が、NIST ガイドラインやその機関のポリシに予め記載されている方法で行われたか、2）計画資料に記されている通りにコントロールが実装されたか、及び 3）システム及び情報のシステムインパクトレベルに対応した適切なモニタリングが継続して行われているか。

モバイル端末（例：スマートホンやタブレット）における特別なセキュリティ要求事項があるか？

データ保護及びリモートアクセスにかかわる既存の連邦政府の全ての要求事項はモバイル端末にも適用される。例えば、OMB 回覧（Circular）A-130 でのセキュリティ要求事項、FIPS 140-2 "*暗号モジュールセキュリティ要件*"、FIPS 199 "*連邦政府情報及び情報システムに対するセキュリティ分類標準*"、及び FIPS 200 "*連邦政府情報及び情報システムに対する最低限順守すべきセキュリティ要求事項*" が適用される（SP 800-53 で指定されている適切なセキュリティコントロールを含む）。各機関は調達プロセスにおけるセキュリティ要求事項を指定して、連邦調達規則 [31]（例：52.225-5 Trade Agreement）の要求事項、OMB 方針（例：M-06-16 及び M-07-16）、及び NIST 標準とガイドラインに則った調達を行っていることを保証すべきである。モバイル端末の使用及び管理に関するさらなるガイダンスは必要に応じて制定される。

---

[31] Federal Acquisition Regulation, https://www.acquisition.gov/?q=browsefar [accessed 8/8/2016].

3.11　OMB 通知文書 M-16-03：2015-2016 年連邦政府情報セキュリティ及びプライバシー管理要求事項に関するガイダンス

OMB 通知文書 M-16-03 は、2015 年初期に行政管理予算局（OMB）及び国家安全保障会議（NSC）スタッフが、体系だった四半期ごとのサイバーセキュリティアセスメントを構築したことを記している。このアセスメントは、機関のサイバーセキュリティ性能を包括的に評価するために、“*重要インフラサイバーセキュリティ改善のための NIST フレームワーク（識別、保護、検知、対応、及び復旧）*”における機能及び関連結果に従って行われる。FISMA 測定基準及び政府機関横断サイバーセキュリティ優先度（CAP）[32]目標による既存の基盤をもとにアセスメントが行われ、当該組織の上位職のリーダーシップによってレビューされる。今後、このアセスメントは、OMB が連邦政府機関のサイバーセキュリティ性能をどのように測定するかの基礎的なイニシアティブになると通知文書に記されている。

[32] *GPRA Modernization Act of 2010, Public Law 111-352,* https://www.performance.gov/cap-goals-list [accessed 8/8/2016].

4 組織的方針

全ての連邦政府組織は、当該組織が収集もしくは生成する情報の取扱いに関する方針を定めている（もしくは定めるべきである）。これには情報管理方針と情報セキュリティ方針が含まれる。暗号技術を使用する組織は、鍵管理方針も合わせて定めるべきである。

4.1 情報管理方針

組織の情報管理方針は、どのような情報が収集もしくは生成されるべきか、及びどのように管理されるべきかを規定する。組織の管理者層は、良い実践の産業標準、組織情報に関する法的要求事項、及び組織が収集したり生成したりする情報を活用して達成しなければならない組織目標を使ってこの方針を構築する。

情報管理方針は、典型的には管理のための役割と責任を規定し、情報管理業務を遂行する人々に必要な権限を確立する。また、どの情報を機微であるとみなし、どのように保護するべきかも規定する。特に、この方針は、認可されてない開示、改ざん又は破棄から保護する必要がある情報の分類を規定する。これらの仕様は、情報セキュリティ方針の基礎をなし、機微情報の分類別に提供しなければならない機密性、完全性、可用性、及び情報源認証の保護のレベルを定める（SP 800-130“*暗号鍵管理システム設計のためのフレームワーク*”参照）。

SP 800-152“*米国連邦政府暗号鍵管理システム用プロファイル*”の 4.1 節では、連邦政府機関のための情報管理方針の内容に求められる要求事項が述べている。

4.2 情報セキュリティ方針

組織の情報セキュリティ方針は、当該組織の情報管理方針の一部を支援、強化するために作成される。これは、懸念される脅威に対してどの情報を保護するべきで、どのような保護が実現されるべきかをより具体的に示す。機微情報の収集、保護、及び配布についてのルールを、紙で行う場合と電子的に行う場合の両方に対して、この方針の中で規定する。情報セキュリティ方針で考慮するものとしては、情報管理方針仕様、当該組織の情報に起こり得るセキュリティ脅威、情報の認可されてない開示、改ざん、破棄又は紛失に伴うリスクなどを含むが、これらに限るものではない。

情報セキュリティ方針として提供するものには、様々な分類の情報に対して付与する情報機微レベル（例：低、中、高）や、情報を保護するための上位レベルのルールが含まれる（*SP 800-130“暗号鍵管理システム設計のためのフレームワーク*”参照）。

SP 800-152 の 4.2 節では、連邦政府機関のための情報セキュリティ方針の内容に対する要求事項が提供されている。

4.3 鍵管理方針

機微情報を保護することを想定する暗号システムを管理する各組織は、組織的方針の宣言に基づいて、当該システムで使用する鍵の管理を行うべきである。鍵管理方針には、認可と保護の目的、暗号鍵材料の生成、配布、アカウント処理、保管、使用、復元及び破棄に適用される制約条件、及び提供される暗号サービス（例：メッセージ認証、デジタル署名及び暗号化）についての記述が含まれる。

鍵管理方針に関するさらに詳しい情報及び要求事項は、SP 800-57 Part2“*鍵管理組織のためのベストプラクティス*”の 3 節で紹介されている。

鍵管理システムは、組織の機微情報を保護するために使用する暗号鍵を管理する。連邦政府組織は独自に鍵管理システムを運営してもよいし、鍵管理サービスと契約してもよい。暗号鍵を管理するための鍵管理システムに関する情報及び要求事項は、SP 800-152 に記されている。

5 リスクマネジメント手順

SP 800-37 “*リスク管理フレームワークを連邦政府情報システムに適用するためのガイド：セキュリティライフサイクルアプローチ*”では、連邦政府情報システムにリスク管理フレームワークを適用するためのガイドラインを提供している。これには、セキュリティ分類[33]、セキュリティコントロール手法の選択や実装、セキュリティコントロール評価、情報システム認可[34]、及びセキュリティコントロール監視といった活動の実行を含む。ガイドラインは以下の目的のために制定された：

- 情報システム関連のセキュリティリスクの管理が、組織のミッション／事業目標、及びリスク対応方針（機能）を通じた上位リーダーシップによって構築される組織全体のリスク戦略と一貫性があることを保証すること
- 必要なセキュリティコントロールを含む情報セキュリティ要求事項が、組織の企業構造及びシステム開発ライフサイクルプロセスに組み込まれていることを保証すること
- （継続的監視を通して）一貫した、十分な情報に基づいた運用中のセキュリティ認可の決定、セキュリティとリスク管理関連の情報の透明性、及び互恵主義[35]を支援すること
- 連邦政府内の情報及び情報システムに適切なリスク軽減戦略を実施することによって、より高い安全性を達成すること

暗号化機能を取り扱う際、情報システムにリスクマネジメントフレームワークを適用するのに関与させるタスクとして、さらに以下の項目に焦点を当てる：

- 情報や情報システムの分類、及びセキュリティコントロールの実装よりもセキュリティコントロールの選択
- セキュリティコントロールの効率性評価
- 情報システムの認可
- 情報システムのセキュリティコントロール及びセキュリティ状態の継続的監視

5.1 情報及び情報システムの分類

情報及び情報システムの分類のために組織として求められることは以下の通りである：

---

[33] FIPS 199 は、国家安全保障システム以外のシステムのセキュリティ分類のガイダンスを提供している。CNSS Instruction 1253 は、国家安全保障システムのための同様のガイダンスを提供している。

[34] システム認可とは、情報システムの運用を認可し、合意された一連のセキュリティコントロールの実施に基づいて、組織の運営や資産、個人、他の組織、及び国家に対するリスクを明示的に受け入れるために、組織の上級責任者が下す正式なマネジメント判断である。

[35] *互恵主義*とは、情報システムのリソースを再利用するために互いのセキュリティ評価を受け入れたり、情報を共有するために互いの評価されたセキュリティ対応を受け入れたりする、参加組織間の相互合意のことである。互恵主義は、透明性がある概念を推進することにより最も上手く達成される（すなわち、情報システムのセキュリティ状態に関する十分な証拠が利用可能であるようにし、当該システム又はそのシステムが処理、保存、伝送する情報の運用及び使用に関して、他の組織の権限を持つ責任者がその証拠を使用して信頼性のあるリスクベースの決定を下すことができるようにする）。

- 情報システムを分類し、FIPS 199、SP 800-30、SP 800-39、SP 800-59、SP 800-60 及び CNSS 命令（Instruction）1253 に記載されているセキュリティ計画にセキュリティ分類の結果を文書化する
- 情報システム（システム境界も含めて）を記述し、その記述をセキュリティ計画に文書化する
- 情報システムを適切な組織のプログラム／管理部署に登録する

5.2 セキュリティコントロールの選定

セキュリティコントロールの選定は以下の手順で行う：

- 組織の情報システムに対する共通のセキュリティコントロールとして、組織が提供するセキュリティコントロールを特定し、セキュリティ計画（もしくは同等の文書）の中に、FIPS 199、FIPS 200、SP 800-30、SP 800-53 及び CNSS 命令（Instruction）1253 に則した形で、当該セキュリティコントロールについて文書化する
- 情報システムのセキュリティコントロールを選定し、FIPS 199、FIPS 200、SP 800-30、SP 800-53 及び CNSS 命令 1253 に記載されているセキュリティ計画に当該コントロールについて文書化する
- SP 800-30、SP 800-39、SP 800-53、SP 800-53A、SP 800-137、及び CNSS 命令 1253 に記載されているように、セキュリティコントロールの有効性、及び情報システムとその運用環境に対するあらゆる変更提案又は実際の変更を継続的に監視するための戦略を策定する
- SP 800-30、SP 800-53、及び CNSS 命令 1253 に則して、セキュリティ計画をレビューし承認する

付録 A：参考文献

1. Public Law 104-113, *National Technology Transfer and Advancement Act of 1995*, 104th Congress, March 7, 1996. https://www.gpo.gov/fdsys/pkg/PLAW-104publ113/contentdetail.html [accessed 8/8/2016].
2. Public Law 107-347, *E-Government Act of 2002*, 107th Congress, December 17, 2002. https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf [accessed 8/8/2016].
3. Public Law 111-5, *American Recovery and Reinvestment Act of 2009*, "Health Information Technology for Economic and Clinical Health Act (HITECH Act)," 111th Congress, February 17, 2009. https://www.gpo.gov/fdsys/pkg/PLAW-111publ5/pdf/PLAW111publ5.pdf [accessed 8/8/2016].
4. Public Law 111-352, *GPRA Modernization Act of 2010*, 111th Congress, January 4, 2011. https://www.gpo.gov/fdsys/pkg/PLAW-111publ352/pdf/PLAW-111publ352.pdf [accessed 8/8/2016].
5. Public Law 113-274, *Cybersecurity Enhancement Act of 2014*, 113th Congress, December 18, 2014. https://www.gpo.gov/fdsys/pkg/PLAW-113publ274/content-detail.html [accessed 8/8/2016].
6. Public Law 113-283, *Federal Information Systems Modernization Act of 2014*, 113th Congress, December 18, 2014. https://www.congress.gov/113/plaws/publ283/PLAW113publ283.pdf [accessed 8/8/2016].
7. *National Institute of Standards and Technology*, Title 15 U.S. Code, Sec. 271 *et seq.*, 2014 ed. https://www.gpo.gov/fdsys/granule/USCODE-2014-title15/USCODE-2014-title15-chap7 [accessed 8/8/2016].
8. *Computer standards program*, Title 15 U.S. Code, Sec. 278g-3, 2014 ed. https://www.gpo.gov/fdsys/granule/USCODE-2014-title15/USCODE-2014-title15-chap7sec278g-3 [accessed 8/8/2016].
9. *Responsibilities for Federal information systems standards*, Title 40 U.S. Code, Sec. 11331, 2014 ed. https://www.gpo.gov/fdsys/granule/USCODE-2014-title40/USCODE-2014-title40subtitleIII-chap113-subchapIII-sec11331 [accessed 8/8/2016].
10. Executive Office of the President, The White House, *Critical Infrastructure Identification, Prioritization, and Protection*, Homeland Security Presidential Directive 7 (HSPD-7), December 17, 2003. https://www.dhs.gov/homeland-security-presidential-directive-7 [accessed 8/8/2016].
11. Executive Office of the President, The White House, *Policies for a Common Identification Standard for Federal Employees and Contractors*, Homeland Security Presidential Directive 12 (HSPD-12), August 27, 2004. https://www.dhs.gov/homeland-security-presidentialdirective-12 [accessed 8/8/2016].
12. Executive Office of the President, The White House, *Improving Critical Infrastructure Cybersecurity*, Executive Order 13636, February 12, 2013. https://federalregister.gov/a/201303915 [accessed 8/8/2016].
13. Executive Office of the President, Office of Management and Budget, *Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities*, OMB Circular Number A-119, Revised, February 10, 1998. https://www.whitehouse.gov/omb/circulars_a119/ [accessed 8/8/2016].
14. Executive Office of the President, Office of Management and Budget, *Managing Information As a Strategic Resource,* OMB Circular Number A-130, Revised, July 28, 2016.

https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised. pdf [accessed 8/8/2016].

15. Executive Office of the President, Office of Management and Budget, *Protection of Sensitive Agency Information*, OMB Memorandum M-06-16, June 23, 2006.

    https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-16.pdf [accessed 8/8/2016].

16. Executive Office of the President, Office of Management and Budget, *Acquisition of Products and Services for Implementation of HSPD-12*, OMB Memorandum M-06-18, June 30, 2006.

    https://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2006/m0618.pdf [accessed 8/8/2016].

17. Executive Office of the President, Office of Management and Budget, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, OMB Memorandum M-07-16, May 27, 2007.

    https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf [accessed 8/8/2016].

18. Executive Office of the President, Office of Management and Budget, *Securing the Federal Government's Domain Name System Infrastruc*ture, OMB Memorandum M-08-23, August 22, 2008. https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2008/m0823.pdf [accessed 8/8/2016].

19. Executive Office of the President, Office of Management and Budget, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, OMB Memorandum M-11-33, September 14, 2011.

    https://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-33.pdf [accessed 8/8/2016].

20. Executive Office of the President, Office of Management and Budget, *Guidance on Federal Information Security and Privacy Management Requirements*, OMB Memorandum M-16-03, October 30, 2015. https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m16-03.pdf [accessed 8/8/2016].

21. Federal Information Processing Standard 140-2 (FIPS 140-2), *Security Requirements for Cryptographic Modules*, National Institute of Standards and Technology, May 2001 (updated 12/3/2002, Change Notice 2). http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf [accessed 8/8/2016].

22. Federal Information Processing Standard 199 (FIPS 199), *Standards for Security*

    Categorization of Federal Information and Information Systems, National Institute of

    Standards and Technology, February 2004.

    http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf [accessed 8/8/2016].

23. Federal Information Processing Standard 200 (FIPS 200), *Minimum Security Requirements for Federal Information and Information Systems*, National Institute of Standards and Technology, March 2006. http://csrc.nist.gov/publications/fips/fips200/FIPS-200-finalmarch.pdf [accessed 8/8/2016].

24. Federal Information Processing Standard 201-2 (FIPS 201-2), *Personal Identity Verification (PIV) of Federal Employees and Contractors*, National Institute of Standards and Technology, April 2013. http://dx.doi.org/10.6028/NIST.FIPS.201-2.

25. National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity,* Version 1.0, February 12, 2015.

http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf [accessed 8/8/2016].

26. National Institute of Standards and Technology, *Guide for Developing Security Plans for Federal Information Systems*, NIST Special Publication 800-18 Rev. 1, February 2006. http://dx.doi.org/10.6028/NIST.SP.800-18r1.

27. National Institute of Standards and Technology, *Guide for Conducting Risk Assessments*, NIST Special Publication 800-30 Rev. 1, September 2012.

http://dx.doi.org/10.6028/NIST.SP.800-30r1.

28. National Institute of Standards and Technology, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, NIST Special Publication 800-37 Rev. 1, February 2010 (updated 6/5/2014).

http://dx.doi.org/10.6028/NIST.SP.800-37r1.

29. National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation: Methods and Techniques*, NIST Special Publication 800-38A, December 2001.

http://dx.doi.org/10.6028/NIST.SP.800-38A.

30. National Institute of Standards and Technology, *Managing Information Security Risk: Organization, Mission, and Information System View*, NIST Special Publication 800-39, March 2011. http://dx.doi.org/10.6028/NIST.SP.800-39.

31. National Institute of Standards and Technology, *Security Guide for Interconnecting Information Technology Systems*, NIST Special Publication 800-47, August 2002.

http://dx.doi.org/10.6028/NIST.SP.800-47.

32. National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53 Rev. 4, April 2013 (updated 1/22/2015). http://dx.doi.org/10.6028/NIST.SP.800-53r4.

33. National Institute of Standards and Technology, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*, NIST Special Publication 800-53A, December 2014 (updated 12/18/2014). http://dx.doi.org/10.6028/NIST.SP.800-53Ar4.

34. National Institute of Standards and Technology, *Recommendation for Key Management, Part 2: Best Practices for Key Management Organization*, NIST Special Publication 800-57 Part 2, August 2005. http://dx.doi.org/10.6028/NIST.SP.800-57p2.

35. National Institute of Standards and Technology, *Guideline for Identifying an Information System as a National Security System*, NIST Special Publication 800-59, August 2003. http://dx.doi.org/10.6028/NIST.SP.800-59.

36. National Institute of Standards and Technology, *Guide for Mapping Types of Information and Information Systems to Security Categories*, NIST Special Publication 800-60 Rev. 1 (2 vols.), August 2008. http://dx.doi.org/10.6028/NIST.SP.800-60v1r1; http://dx.doi.org/10.6028/NIST.SP.800-60v2r1.

37. National Institute of Standards and Technology, *Electronic Authentication Guideline*, NIST Special Publication 800-63-2, August 2013. http://dx.doi.org/10.6028/NIST.SP.800-63-2.

38. National Institute of Standards and Technology, *Interfaces for Personal Identity Verification*, NIST Special Publication 800-73-4, May 2015 (updated 2/8/2016).

http://dx.doi.org/10.6028/NIST.SP.800-73-4.

39. National Institute of Standards and Technology, *Biometric Specifications for Personal Identity Verification*, NIST Special Publication 800-76-2, July 2013.

    http://dx.doi.org/10.6028/NIST.SP.800-76-2.

40. National Institute of Standards and Technology, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, NIST Special Publication 800-78-4, May 2015.

    http://dx.doi.org/10.6028/NIST.SP.800-78-4.

41. National Institute of Standards and Technology, *Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)*, NIST Special Publication 800-79-2, July 2015. http://dx.doi.org/10.6028/NIST.SP.800-79-2.

42. National Institute of Standards and Technology, *Secure Domain Name System (DNS) Deployment Guide*, NIST Special Publication 800-81-2, September 2013.

    http://dx.doi.org/10.6028/NIST.SP.800-81-2.

43. National Institute of Standards and Technology, *PIV Card Application and Middleware Interface Test Guidelines (SP 800-73-4 Compliance)*, NIST Special Publication 800-85A-4, April 2016. http://dx.doi.org/10.6028/NIST.SP.800-85A-4.

44. National Institute of Standards and Technology, *Guidelines for Media Sanitization*, NIST Special Publication 800-88 Rev. 1, December 2014. http://dx.doi.org/10.6028/NIST.SP.80088r1.

45. National Institute of Standards and Technology, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*, NIST Special Publication 800-116, November 2008. http://dx.doi.org/10.6028/NIST.SP.800-116.

46. National Institute of Standards and Technology, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, NIST Special Publication 800-122, April 2010. http://dx.doi.org/10.6028/NIST.SP.800-122.

47. National Institute of Standards and Technology, *A Framework for Designing Cryptographic Key Management Systems*, NIST Special Publication 800-130, August 2013.

    http://dx.doi.org/10.6028/NIST.SP.800-130.

48. National Institute of Standards and Technology, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, NIST Special Publication 800137, September 2011. http://dx.doi.org/10.6028/NIST.SP.800-137.

49. National Institute of Standards and Technology, *A Profile for U. S. Federal Cryptographic Key Management Systems (CKMS)*, NIST Special Publication 800-152, October 2015. http://dx.doi.org/10.6028/NIST.SP.800-152.

50. National Institute of Standards and Technology, *Guidelines for Derived Personal Identity Verification (PIV) Credentials*, NIST Special Publication 800-157, December 2014.

    http://dx.doi.org/10.6028/NIST.SP.800-157.

51. National Institute of Standards and Technology, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, NIST Special Publication 800-161, April 2015. http://dx.doi.org/10.6028/NIST.SP.800-161.

52. National Institute of Standards and Technology, *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*, NIST Special Publication 800-162, January 2014. http://dx.doi.org/10.6028/NIST.SP.800-162.

53. National Institute of Standards and Technology, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, NIST Special Publication 800-171, June 2015 (updated 1/14/2016). http://dx.doi.org/10.6028/NIST.SP.800-171.

54. National Institute of Standards and Technology, *Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms*, NIST Special Publication 800-175B, August 2016. http://dx.doi.org/10.6028/NIST.SP.800-175B.

55. Committee on National Security Systems (CNSS), *Security Categorization and Control Selection for National Security Systems*, CNSS Instruction 1253, March 27, 2014. Available at: https://www.cnss.gov/CNSS/issuances/Instructions.cfm [accessed 8/8/2016].

56. National Institute of Standards and Technology, and the Communications Security Establishment Canada, *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program,* CMVP, March 28, 2003, Last Update June 17, 2016. http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf [accessed 8/8/2016].

57. National Institute of Standards and Technology, *Supplemental Guidance on Ongoing Authorization: Transitioning to Near Real-Time Risk Management*, June 2014. http://csrc.nist.gov/publications/nistpubs/800-37-rev1/nist_oa_guidance.pdf [accessed 8/8/2016].