平成 28 年度製造基盤技術実態等調査

我が国の技術情報保全強化に関する調査

平成 29 年 3 月

株式会社アイ・ビー・ティ

はじめに

■本事業の目的

民生技術と防衛装備技術のボーダレスが進む中で、産業競争力上重要な技術を適切に管理することは、我が国として産業競争力の源泉となる技術力を維持していくことのみならず、安全保障の面からも重要となっている。

これまで、我が国は、企業等の技術を保全する枠組みとして、「不正競争防止法」や「営業秘密指針」、「情報セキュリティマネジメント（ISMS: Information Security Management System）」等、各種のルールを整備してきたところである。このような現行ルールを総合的に勘案しつつ、政府から受領する機密情報、企業等における営業秘密、秘密情報等の取扱、物的措置・人的措置等の観点から、企業等における技術情報の管理の在り方について検討を深めていくための基礎資料を整備することを目的とする。

■背景と問題意識

我が国ではこれまで、武器輸出三原則等の影響もあり、国家安全保障に係わる分野における海外展開経験に乏しく、外国政府から渡された機密情報の適切な管理の在り方について充分な知見を持ち合わせておらず、米国や NATO 諸国のように、厳格かつ総合的な産業保全に関する制度やルールが確立されていない状況にある。下表の通り、我が国にも企業等の保有する技術を管理するための幾つかの枠組みは存在しているが、これらは、必ずしも企業向けの産業保全のあり方を意図して制定されたものではなく、米国の国家産業保全プログラム運用マニュアル（NIISPOM）等とは観点や視点が異なっている。

【現行の日本の制度・ルール例と NISPOM との比較】

ルール名称	特徴と NISPOM との比較
特定秘密の保護に関する法律	日本の安全保障に関する情報のうち特に秘匿することが必要であるものを「特定秘密」として指定し、取扱者の適性評価の実施や漏えいした場合の罰則などを定めた日本の法律。通称は特定秘密保護法。
	特徴：特定秘密の取扱者についての言及
営業秘密管理指針	経済産業省が不正競争防止法を所管し、また TRIPS 協定など通商協定を所掌する行政の立場から、企業実務において課題となってきた営業秘密の定義等（不正競争防止法による保護を受けるための要件など）について、イノベーションの推進、海外の動向や国内外の裁判例等を踏まえて、一つの考え方を示すもの。法的拘束力を持つものではない。
	特徴：NISPOM とは意味づけが異なり、法律としての構成要件の説明となる側面が強い。
情報マネジメント標準(ISMS)	情報技術（セキュリティ技術）情報セキュリティ管理策の実践のための規範。

	特徴:JIS であり政府下請限定ではないが、内容項目としては NISPOM に近い。

■事業内容

以上の事業目的および背景・問題意識を踏まえ、本事業では、(1) 企業における情報管理の実態調査、(2) 技術情報の管理の在り方を検討するための会議の開催、(3) 文献調査（国内外の情報保全に関するルールの収集・整理）を実施し、(4) 我が国の情報保全制度の在り方の方向性を整理し、本報告書を取り纏めた。

1.　企業における情報管理の実態調査

情報保全の専門家 7 名、企業 16 社、関連組織・研究機関 3 件を対象にヒアリング調査を実施し、企業における情報管理の実態について幅広く情報を収集した。ヒアリング調査の実施要領と結果は以下の通りである[1]。

■実施目的

我が国の産業競争力上重要な技術等の情報保全制度の強化を目指している中で、現状の企業における情報保全に対する取り組み等の実態について把握し、我が国における技術情報の管理の在り方を検討する際の参考とすること。

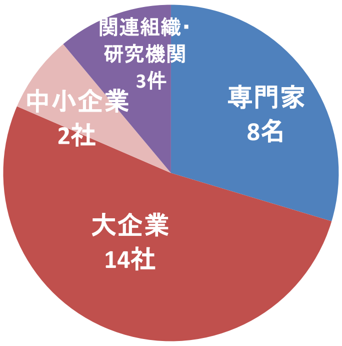
■実施期間：2017 年 1 月～3 月

■実施方法：訪問による面談およびメール（回答表）

■調査対象：

①重要技術を保有すると想定される日本企業 16 社
（資本金 3 億円以上の大企業 14 社、
3 億円未満の中小・中堅企業 2 社）

②情報保全の専門家 8 名
関連組織・研究機関 3 件



■調査内容：

①企業に対しては、企業における技術情報保全についての運用の実態、課題や問題等を把握するため、以下の内容に沿ってヒアリング調査を行った。

技術情報の管理に係わる社内体制		
	●技術情報の管理に係わる社内体制のあり方について、何か規定はあるか。（自社向け及び/または下請け企業向け）	
情報保全に関する社内ルールやマニュアルの整備		
	●情報保全に関する社内ルールやマニュアル（成文化されたもの）があるか。	
	→有の場合：	●参照しているガイドラインはあるか。どのような項目があるのか。
		●社内全体で均一のものか、部署によって多少の違いがあるのか。 【親会社/子会社】 ●子会社を含むグループ会社全体の技術情報を管理するものか、親会社単独のものか。 ●子会社の情報管理はどのように徹底させているのか。 【元請/下請企業】 ●元請企業：下請け企業の情報管理の状況について、どの程度把握しているか。チェック頻度やチェックの際の項目はどのようなものか。

[1] 個別企業名や機微な情報を含むため、本公開版報告書では概要のみを記載している。

	●下請企業：ヒヤリ・ハット事例やインシデント事例をどのように情報保全ルール（もしあれば）に反映させているのか。主力の従業員（職人）の人材流出（ヘッドハンティング）をどのように防止しているのか。
	●どのくらいの頻度で、どの程度の細部まで、見直し・更新を行っているのか。
→無の場合：	●皆がわかっていて慣習的に運用していることはあるのか
技術情報の管理区分	
●社内で技術情報の管理を行う際、独自の情報保全区分（丸秘、秘、極秘など）を設定しているか。	
→有の場合：	●どういった区分があり、それぞれどのような基準で分かれているのか。
	●区分を指定するのは誰か。 ●情報保全指定の解除または格下げといった判断は、誰がどういった基準で行っているのか。
技術情報の保全	
(1) 人及び施設に対するセキュリティ・クリアランス（※）	
●人及び施設に対して、クリアランスを社内（及び子会社）で及び/または下請け企業に対して実施しているか。 ●第三者（例えば防衛省など）から人及び施設に対するクリアランスを受けているか。	
→有の場合：	●どういった区分があるか ●クリアランスを与える/受ける際の調査事項と調査方法はどのようなものか ●クリアランスの有効期限はどれくらいか ●付与した/されたクリアランスの監査・認証は行われているのか ●負担は感じているか（どのような負担があるのか(費用、時間、労力)）。
(2) その他、技術情報保全のための取り組み・工夫等	
●技術情報の保全に対して、どの程度の投資・努力を行っているか。 ●情報管理のチェック機能として、どのような体制を敷いているのか。	
不正に対する対応	
●不正を迅速に発見するための対策等は講じているのか。 ●違反等を確認した場合、どのように対処しているか。 ●罰則や報告義務等はあるか。	
他組織との相互認証	
●他組織との間で、技術情報の管理区分やクリアランス等の相互認証を行っているか。	
人材育成の仕組み	
●社内及び子会社や下請け企業等において、情報保全のモニタリング要員等の人材を育成するため、技術情報管理に関する教育や訓練等を実施しているか。	
→有の場合：	●どのくらいの頻度で行っているのか。 ●それは制度としてあるのか、それとも風土として実施されているのか。
その他	

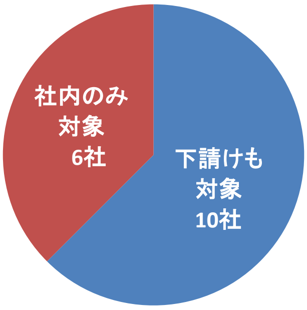
(※) セキュリティ・クリアランス＝秘密情報取扱いにあたって特定の要件を満たしているかの適格性確認（あるいはそれに近い仕組み）

②企業以外（専門家、関連組織等）に対しては、我が国の情報保全の在り方に関する課題、今後の方向性等について各々の立場に基づく幅広い意見を収集した。

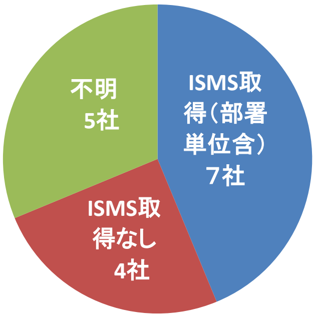
■企業 16 社に関するヒアリング結果の概要

- 情報保全に関する社内体制
  - ➢ 大企業の場合は、全社統一基準を設けた上で個々の事業部やカンパニーの事業内容に応じた規定やマニュアルを定めて運用している場合が多い。
  - ➢ 全ての企業で情報保全の必要性、深刻性を認識し、強化の方向に向いていた。

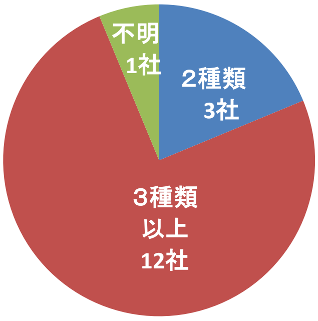
- 情報保全に関するルール・マニュアル
  - ➢ 社内規定はグループ会社全社にも適応していた。
  - ➢ 下請け企業にも同じルールやマニュアルを適応する場合は、半数以下であった。下請けに適応しない場合も、現場に即し内容を緩和したもので運用していた。
  - ➢ 下請けにまでルールを遵守させるにはコスト面も含めて難しい。
  - ➢ 国が何らかの指針を示してくれると後押しになる。
  - ➢ 経産省のハンドブック等を参考にして作成したものもあった。



- ISMS の認証
  - ➢ 認証は取得していないが、運用時の参考にしている企業が２社あった。
  - ➢ 取得企業は ISMS のガイドラインに沿って運用している。
  - ➢ 取得しないうちの１社は維持コストや手間を考慮すると、踏み切れずにいる。



- 技術情報の管理区分



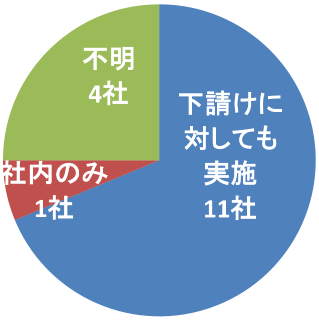
※３種類以上：3～5 種類。

  - ➢ 極秘、秘、社外秘、関係者外秘等、企業によって名称は様々。
  - ➢ １社はインサイダー取引に関する情報等、明確な分類規定があった。
  - ➢ ４種類に分かれているが、その差は曖昧という回答もあった。
  - ➢ 管理区分の決定は、基本的に部門長。
  - ➢ 判断基準が個人の裁量に依存する場合もあり、明確

な基準が必要と感じる。

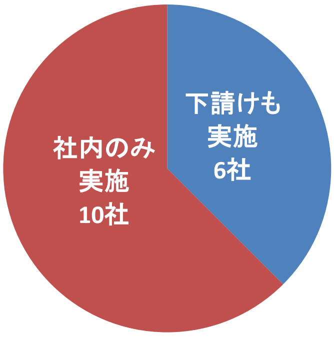
- 人の管理
  - 外部の認証機関の認証を受けているところはなかった。
  - 入社時、特定部門への異動の際に秘密保持契約を締結している。
  - 性善説で運用と発言した社が半数程度。

- 施設のクリアランス
  - 防衛省以外から自社がクリアランスを受けている事例は聞かなかった。外部機関の認証取得がアクセス権の条件になっている企業はなかった。
  - 自社の施設管理として、金庫やキャビネットへの施錠、入退室管理について濃淡はあるが全ての社で実施していた。

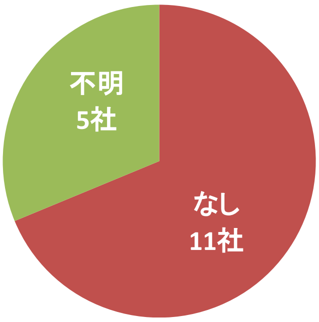


- 情報の管理
  - すべての社がサーバーにはアクセスコントロールをかけていた。アクセス権は、役職ではなく Need to know 判断による。
  - 社支給の PC やモバイル、USB メモリしか使用できない社が多い。
  - 社外からのリモートアクセスについてもセキュリティは確保されていた。
  - メールの扱いも重要。スマホの規制は今後の課題という企業が多かった。

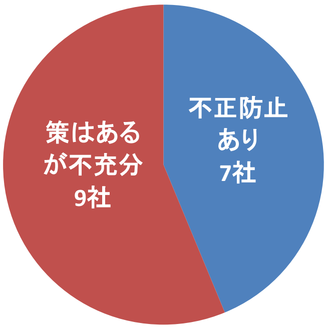
- 人材育成
  - 全ての社で何らかの人材育成/教育を実施していた。下請けも全て対象としている社は1/3 程度。
  - e-learning、セルフチェック、各種講習会、コンプライアンス教育等。
  - 年 1 回程度という回答が多い。不定期の場合もあった。



- 相互認証
  - 防衛関連では一部あると聞いているが不明。



- 不正防止対策
  - 監視カメラ、入室や休日出勤時の複数体制、等。
  - 社内に専用相談窓口を設置している。
  - 事故の場合は懲戒免処分の対象とすることを就業規則に定めている。
  - 内部監査を実施している企業は半数程度。
  - 整備が充分でなく悪意をもっての不正が可能な状況にあるとの回答もあった。
  - 退職者対策として退職時の秘密保持契約している社が多い。



- その他
  - 技術情報保全の在り方は過渡期にあり、戸惑うことが多い。
  - IT 化が進む中、情報管理の方向性に迷いは生じやすい。
  - 個人の情報管理を徹底させるためには強制力を伴う方策が必要。
  - 企業として情報に関する体系的な法整備が求められている。
  - アクセス制限は容易に行えるが、アクセスできる人を管理することは困難。
  - 取引先に対する情報保全体制の懸念や下請け企業への管理強化など社外への強化促進は難しい。
  - サイバーセキュリティ対策はコストが膨大で 1 社だけでは負担できず、官民協力が必要。
  - 単に管理強化するだけでなく、企業としては収益確保と経済活動への支障を抑える工夫が必要。
  - 一部企業は SP-800-171 を含む米国法への対応を課題として感じている。
  - 人を介しての流出防止策としては、違反時の罰則規定よりも情報保全に関する会社内のインセンティブ（報酬、役職等）を高める方が有効に感じることがある。

今回のヒアリングは大手メーカーが中心であったため、全般的に需要な技術情報保全の重要性について充分に認識しており、各社ともに様々な取り組みを実施していた。しかし、未だ不十分と感じるところがあるとの意見も同時に聞くこととなった。

今後は、性善説ではなく性悪説に立った情報漏えい対策に対する社会的啓蒙の必要性や、国が「あるべき情報管理の姿」を示すガイドラインや指針を提示してくれれば、自社が今後進むべき情報保全の方向性も明確になるという意見が複数からあがっていた。また、国のインフラ整備として日本版クラウド構築について取り組んでほしいという意見もあった。

2.　技術情報の管理の在り方に関する有識者会議の開催

国内の安全保障に関する学識経験者、輸出管理に関する学識経験者などから構成される検討会「我が国の技術情報保全の在り方に関する検討委員会」を設置、我が国の技術力の維持の観点から、委員それぞれの見解と立場をもって、現行ルールを踏まえつつ、技術情報管理の在り方について、現状の課題と今後の方向性等を含め幅広く検討した。

■目的

我が国には、企業等の技術を保全する枠組みとして「不正競争防止法」や「営業秘密指針」、「情報セキュリティマネジメント」など各種のルールが存在するが、今後このような現行ルールを総合的に勘案しつつ、政府から受領する機密情報、企業等における技術情報の管理の在り方について検討を深めていく必要がある。そこで本委員会の目的は、技術力の維持の観点から、我が国の技術情報管理の在り方について、幅広く検討するものである。

■進め方の特徴

企業における情報管理の実態調査（本稿 1.）および国内外の情報保全に関するルール整理（本稿 3.）の結果について、また経済産業省の現行政策の状況も踏まえて議論を行った。

■実施時期と回数

2017 年 1 月～3 月の期間中、全 3 回の会議を開催した。1 回ごとの会議時間も充分に確保した。

■委員：８名

委員長

株式会社グローバルセキュリティ　代表取締役	山崎　剛美氏

委員（あいうえお順）

英知法律事務所　弁護士	岡村　久道氏
経団連地裁委員会企画部会委員、三菱電機　知財センター長	木全　政弘氏
公益財団法人未来工学研究所　研究参与	西山　淳一氏
情報セキュリティ大学院大学　教授	原田　要之助氏
㈱富士通システム統合研究所　安全保障研究所　特任研究員	二俣　晃治氏
防衛基盤整備協会　理事	古川　明氏
新日鉄住金株式会社　知的財産部　戦略推進室長	矢田部　英爾氏

■経済産業省の参加者

　経済産業省から関係者約20名がオブザーバーとして当会に参加し、意見交換と情報共有を行った。

2.1.　第１回委員会

■実施要領

日程：2017年１月12日（木）15:00-17:00

場所：経済産業省別館１階　105会議室

次第：	①開会の挨拶	経済産業省
	②出席者紹介	事務局
	③委員会の取扱いについての確認	事務局
	④重要技術管理政策について	製造産業技術戦略室
	⑤委員長の互選	
	⑥資料説明	事務局
	⑦各委員のコメント・意見交換	各委員
	⑧事務連絡(今後のスケジュール)	事務局

■テーマ

我が国の情報保全の現状および課題の整理

■主な議論内容

●技術情報保全に関する現状と課題

- 現在起きている情報保全に関する事象は、サイバーセキュリティと内部不正という二系統の問題に起因している。
- 高度な技術のための情報保全／管理に関しては社内で一定の基準があるが、それが発明者、開発者の意識レベルで共有できているかは疑問に感じる。
- 製造設備のリモートメンテによる継続的な漏えいリスクや、提供ベンダーの新機能追加によるリスク等の新たな脅威に対して充分に対応できていないのではないか。
- 企業単体ではなく、子会社も含めたサプライチェーン全体としてのサイバーセキュリティを考えるべき。
- 情報保全の責任者の専任としっかりした権限を持たせることが必要。
- 保全すべき技術情報の対象にはハードとソフトの両面があり、リバースエンジニアリングも含めて対応を考える必要がある。
- 脅威に対応するためのツールが国産品でないことは問題ではないか。
- 最近は汎用品に対するセキュリティ要求も高まる傾向にあり、「管理すべき秘密でない情報（CUI：Controlled Unclassified Information）」の保全についても一定の基準が必要ではないか。

●情報保全に係る企業負担増大の懸念

- 企業に自社の営業秘密以外の情報保全を要請する場合、企業側としては管理の負担が増え不満に繋がるのではないか。
- 防衛省向け事業の場合は、政府が設備投資等のコストを負担してくれるが、防衛省以外の場合には政府の負担はなく、企業としては保全基準と設備投資の負担とのバランスを考えなければならない。

●情報保全に係る制度・ルールの状況

- 防衛・民生の技術のボーダレス化を踏まえて、米国の NISPOM（National Industry Security Program Operation Manual）や特定防衛秘密等の防衛関連の情報保全のしかたも参考になるのではないか。

●用語定義の必要性

- 情報保全に関する用語の整理は未だ不充分な部分もあり、少なくとも本委員会では統一しておく必要がある。例えば、「クリアランス」、「情報保全の区分」、「機密と秘密」等。

●情報保全強化に伴い生じる課題

- 防衛分野に関しては厳重に管理される仕組みがあり、秘密に指定された情報が漏れることはまずありえない。ただしその結果、社内ですら情報共有ができず開発が遅れをとるという危惧がある。防衛分野に関しては基準を守ることも大事だが、要件をある程度緩和して開発をエンカレッジさせるようにしたいとも感じている。

●強化に向けた観点

- 情報は漏えいするという事故前提社会という考えに立って、対応を考えるべきではないか。
- 情報漏えいを防ぐにあたっては、“人と知りあう”ということ自身にも注意が必要というような「入口」から啓蒙する必要がある。

2.2.　第２回委員会

■実施要領

日程：2017年2月14日（火）10:00-12:00

場所：経済産業省別館１階　114　会議室

次第：①本日の議事およびテーマについての説明	委員長
②プレゼンテーション	
経済産業省の関連施策	経済産業省
情報保全に関する企業実態	二俣晃治氏
③企業実態調査の中間報告	事務局
④文献調査報告	
NISPOMと国内ルールとの比較	事務局
⑤ディスカッション	委員長
⑥今後の方向性についての説明	経済産業省

■テーマ

技術情報保全に関する実態把握

■主な議論内容

●技術情報保全に関する政府の取り組みの現況と意見

○　技術流出防止（外為法）について

・輸出管理内部規定には大学も対象に含まれる。

・海外の留学生や、日本に居住、帰化した者に差別がないようにすると同時に、帰国する場合に、みなし輸出に該当しないよう注意が必要ではないか。

・インターネットを介した無体物の輸出も脅威となるのではないか。

○　営業秘密ハンドブックについて

・情報漏えいについて、中小企業や大学の防止策のレベルが懸念される。

・営業秘密の対象について誰が決定し、漏れたことをいかに証明するかは課題である。

○　サイバーセキュリティの取組みについて

・個人情報と重要技術情報とを一律に語るのではなく、それぞれの価値に立脚して守り方を考えるべき。

●企業における技術情報保全の実態

・対象企業は全般的に社内ルールやマニュアルを定め重要情報を慎重に管理していた。

・多くの企業では基本的に性善説に基づいた規約やルールとなっていた。

・防衛と民生技術のボーダレス化が進む中で、全社的な意識向上が求められている状況

にある。

・個人個人の情報管理を徹底させるために強制力のある方策があれば有難いという意見もあった。

●米国 NISPOM と国内ルールとの比較

・NISPOM の概略を説明し、情報保護ハンドブックと ISMS と比較した上で NISPOM の位置づけに関する調査結果を報告。

・３件のルールについて、分析軸（組織体制、組織としてのマニュアル作成の要不要および項目、秘密情報の指定と解除等、クリアランス、秘密情報の管理、他組織との相互認証、人材育成の取組）に沿って整理を行った。

●情報保全の企業実態に関する意見

○企業における情報保全の今後の課題

・秘密に関する要求事項と推奨事項とは明確に分けて考えるべきではないか。

・オープン・クローズについて最近は整理が難しくなっている。あえて特許化せずに秘密にする方法もある。逆にリソースを有効活用する観点から、社内では共有することも必要になってきている。

○情報保全に関する何らかの基準の必要性

・日本のハンドブックは強制力がないが、NISPOM には強制力があるという点で大きく異なっている。

・大学での研究に関する情報の保護も重要な課題である。

・秘密の管理レベルは、最もコストをかけている防衛関連の秘密管理レベル、大企業の管理レベル、大学や中小企業の管理レベルの３つに大別できる。防衛関連と大企業の中間レベルくらいの基準が整備されるとよいのではないか。一方で、大学や中小企業が対応できるレベルも必要と思う。

・セキュリティに関する費用はコストではなく将来に向けた投資であると捉えるものではないか。

●今後の進め方（経済産業省）

・委員会での議論を通じて「民生技術と防衛技術のボーダレス化の進展に伴い、中間領域の情報種皮管理の在り方を考えることが重要」、「技術情報の保全に関する何らかの基準が必要」等の論点が提起された。

・企業等における情報管理・保全の実態調査を行っているところ、これらの内容も踏まえ、企業等が情報管理・保全の仕組みの構築または改善する上で参考となるような情報管理・保全に関する考え方を整理する。

・当該整理にあたっては、情報管理と活用・コストとのバランスや、既に企業で参照・

活用されている各種の既存ルールとの整合を考慮しつつ、特に重要な技術の情報の保護を確実にするための措置（人のアクセス制限や具体的な物理的保護措置、サイバーセキュリティ）の具体化等について検討を行う。

2.3.　第 3 回委員会

■実施要領

日程：3/15（水）10：00-12：00

場所：経済産業省別館 1 階　108　会議室

次第：	①開会の挨拶	経済産業省
	②本日の議事およびテーマについての説明	委員長
	③企業実態調査報告	事務局
	④プレゼンテーション	
	情報セキュリティの取組みと課題	木全政弘氏
	技術流出防止に関する取組み	矢田部英爾氏
	技術情報保全に関する人材育成	古川明氏、小島和浩氏、浅見政博氏
	⑤プレゼンテーション	
	重要技術の適切な情報の管理等に向けた考え方について	経済産業省
	⑥ディスカッション	
	⑦総括	委員長
	⑥閉会の挨拶	経済産業省

■テーマ

我が国の技術情報保全の在り方に関する方向性

■主な議論内容

●企業における技術情報保全の運用実態の調査結果

・今回ヒアリングを実施した全企業においては、技術情報保全の重要性を認識し、各社で何らかのルール・マニュアルを整備し保全に努めていた。

・技術情報保全の在り方や方向性については、様々な課題を感じている企業が複数社あった。国として「あるべき情報管理の姿」を示すガイドや指針を提示してほしいという意見も聞かれた。

●今後の企業における重要技術情報保全の在り方に関する意見交換

○　秘密レベルのラベリングが重要。重要情報を洗い出し、ランク付け、ラベリングを誰がどういう方法で行うのか。

○　中小企業や大学等研究機関が大企業と同等に技術情報を管理していくことは困難であり、何らかの支援が必要。

・特にベンチャー企業に対してはサポートする組織が必要ではないか。

・中小企業が対応できない最大の理由は、システムセキュリティのレベルアップにコス

トと専門性が必要ということ。

○　安全なクラウドサービスの構築が求められる。

・充分なセキュリティを確保したクラウドサービスがあれば、中小企業、ベンチャー、大学、研究機関でも保全しやすい体制を構築できるのではないか。

・クラウドは、利便性が高いものだが、安全性の観点から国内に設置すべきではないか。

○　メールのセキュリティを確保するには、個人による暗号化ではなく送信時に自動的に暗号化するシステムがスタンダードになりつつある。

○　情報共有のためにはセーフティネットワークパスの構築が望ましい。

・CUI レベルのためのセキュアな官民ネットワークの構築を検討してもらいたい。コスト負担の問題はあるが、信頼性パスで結ばれると官民、民間同士でも利便性が高まる。

・アクセス権を分別するグループ認証の技術開発も進んでいる。

○　CSIRT 協議会、フィッシング対策協議会等のネットワークを活用した民民の最新情報交換は有効な手段の一つになると思われる。

●「重要技術の適切な情報の管理等に向けた考え方」について意見交換

○　ガイドラインを活用するための具体的な施策が必要であろう。

○　国籍に関する条項も加えていただきたい。

○　特にデュアルユースの場合、ガイドラインと企業の規則との整合性が必要となる。守りすぎず緩すぎずといったバランスが大切だろう。

○　トレーニングの対象は中間管理職以上のコア人材に実施することにしてはどうか。

3.　国内外の情報保全に関するルール

3.1.　我が国において技術を保全するための枠組み

近年、重要技術を適切に管理することは、我が国として産業競争力の源泉となる技術力を維持するためにも重要との認識が拡大している。我が国においては国家の秘密を直接保護する法律は長らくなかった。公的な秘密を保護する法律としては国家公務員法や自衛隊法の中で一部触れられているに留まっていた。こういった中で平成25年12月13日「我が国の安全保障に関する情報のうち特に秘匿することが必要であるものの保護に関し、必要な事項を定め」（内閣府）た「特定秘密の保護に関する法律」が公布され初めて国家の秘密保護の法制度が整えられた。

従って我が国の重要技術情報の保護はもっぱら、民間の営業秘密を守る法律としての不正競争防止法による保護に頼ってきた。

例外的に、日米間における相互防衛援助協定が締結されたことを受けて、日米相互防衛援助協定等に伴う秘密保護法が制定されており、防衛省はこれら（日米相互防衛援助協定等に伴う秘密保護法、特定秘密の保護に関する法律、自衛隊法）に基づき、民間との協力に関しても各法律を守る為の特約条項をその契約に含め、これらに関する技術情報の保全に努めている。

また、これとは別にIT技術の進展に伴い情報セキュリティの必要性が世界的に高まり、我が国も世界各国と協力して情報セキュリティの世界標準であるISO/IEC27002を制定し、これを国内標準としてJIS化も行ってきた。防衛省においてもこれに則った形で特約条項「装備品等及び役務の調達における情報セキュリティの確保に関する特約条項」を設けて情報セキュリティの徹底を務めさせている。

我が国における各種秘密とその根拠法・官民の契約条項・ガイドの位置づけを示した図は、次頁の通りである。

【日本の各種秘密とその根拠法・官民の契約条項・ガイドの位置づけ】

	国家				民間	共通	
秘密	特定秘密	特別防衛秘密	(省)秘密		営業秘密	個人情報	情報システム
法律	特定秘密保護法	MDA法	自衛隊法	国家公務員法	不正競争防止法	個人情報保護法	
契約	特定秘密の保護に関する特約条項	特別防衛秘密の保護に関する特約条項	秘密保全に関する特約条項				情報セキュリティの確保に関する特約条項
ガイド					秘密情報の保護ハンドブック		ISMS

なお、「秘密情報の保護ハンドブック」および「ISMS」を米国 NISPOM と比較した表を本稿「4.我が国の技術情報保全の在り方の方向性」に掲載している。

3.2.　米国における関連ルール

3.2.1.　NISPOM の法的背景と関連組織

1993 年 1 月にブッシュ大統領が署名した大統領令 12829 は「国益の増進、米国政府機関に関する契約とライセンスの円滑化、および政府以外への権限受領を促進すること」を目的とする。このためには、機密情報へのアクセスを必要とする場合、国家安全保障上、この情報が行政府内での保護と同等の方法で保護される必要があり、同時にまた国家安全保障は、我が国の産業セキュリティ･プログラムが、米国の経済的･技術的利益を促進することを求めている。冗長化、重複、または不必要な要求は、こういった利益を阻害するものである。したがって、国家産業セキュリティ･プログラムは、機密情報を保護し、我々の国家の経済的･技術的な利益を維持するため、単一の、統合された、まとまりのある産業セキュリティ･プログラムとして提供されなければならない。」と宣言している。なおこれ以前は、1960 年の大統領令 10865（EO 10865）が産業内の機密情報を扱っていた。EO 10865 は、機密情報が契約の入札又は落札プロセスを通じて、民間部門に提供することができる方法を規制していた。

NISP では、機密契約向けのセキュリティ要件をより均一にする目標で、以下に 4 つの主要原則を示している。

- セキュリティ手順の均一性の実現
- セキュリティ手順で互恵契約の原則の実装[2]、特に施設や人員クリアランス
- 重複や不要な要件の排除、特に機関による審査
- セキュリティコストの削減

米国政府は、これらの原則に基づき民間企業に対する機密文書の公開の必要性を審議し監督する。この計画方針の決定権は国家安全保障会議にあるが、遂行の権利は ISOO 局長が持つ。ISOO の責務は次の通り。

- NISP の実装と監視
- 大統領令 12829 を確実に遵守させるため省庁、請負業者、ライセンス及び権限付与者

[2] 互恵契約（reciprocity）とは、情報システムリソースの再利用や、互いのセキュリティ状態の評価結果を受け入れることによる情報の共有を目的として、参加している組織間で、互いのセキュリティアセスメント結果を受け入れることに合意することをいう。互恵契約(reciprocity)を成立させる最良の方法は、透明性の概念を促進することである（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を誰もが入手できるようにすることによって、別組織の運用認可責任者がその証拠を利用して、そのシステム、または、そのシステムが処理、格納、もしくは伝送する情報の運用および使用に関して信頼のおけるリスクベースの意思決定を下せるようにする。）

の行動の監督。

- 法令、内部ルール、ガイドラインを実装する全機関のレビュー
- 機密情報へのアクセスや保管を行う各省庁、請負業者、ライセンス及び権限付与者によるNISPの実装のオンサイトレビューの実施。
- NISPの実施について毎年大統領への報告。
- 1995年のEO 12958「国家安全保障に関する機密情報」に基づいて設立され米国政府全体の機密分類プログラムの監督
- 国家安全保障会議を通じて大統領に機密分類の政策変更を勧告

また、大統領令12829は、国家産業セキュリティ・プログラム政策諮問委員会（NISPPAC）を設立している。NISPPACは、政策立案における政府と産業界の間の真のパートナーシップを体現し、政府と産業界双方からの代表が、その変更への勧告を含めて NISP のポリシーに関するすべての事項について議長に就任するISOO局長に助言を与える。

現在のように政府関係の人的クリアランスが一元化されたのはビル・クリントン大統領によって1995年8月4日に署名され大統領令12968によってである。EO 12968の主な規定では、以下としている。

- Need-to-Knowが確認された人員以外機密情報へのアクセス権は付与されない
- 国家安全保障の利益と明らかに一致している従業員が、機密情報へのアクセスを確保するための効果的なプログラムを確立し維持する責任は、各省庁の長官にある。
- 適切な身元調査に基づいて省庁の長官または指名を受けた職員によって有利な裁定を受けた場合を除き従業員が機密情報へのアクセス権を付与されてはならない。
- 連邦政府機関に対し、認可された捜査機関または裁定機関によって完成されているセキュリティ・クリアランスの背景調査と決定を受け入れることを求める。（互恵原則）

更にブッシュ大統領による2008年の大統領令13467 では、人的クリアランスを規定するとともに、そのバックボーンとなる機密情報適格性判断の統一基準策定並びにEO12968での適格性審査機関指定の最終権限者が国家情報長官室（ODNI）の管理下にまかされることとなった。

オバマ大統領は、「機密情報及び政府管理情報」[3]と題された覚書を2009年5月 27 日に公表し、機密指定制度の改革に乗りだしている。

- 国家機密解除センターの設立

[3] Classified Information and Controlled Unclassified Information
http://www.whitehouse.gov/the_press_office/Presidential-Memorandum-Classified-Information-and-Controlled-Unclassified-Information

- "機密上"の問題に対処し、機密指定の説明責任を向上させる有効な手段
- 機密情報の共有化の促進
- 適切な権限の下で機密が解除され一般に公開されたものの再機密禁止
- 電子環境への配慮（例えば、電子情報システム上の情報の保護）
- 政府の正当な利益に必要な保護を提供しながらの開放性と透明性

同覚書では後日、機密指定制度と政府管理情報に関する新たな大統領令を出すために、関連する行政機関に対し、改革案の提出を求めている。

その後2009年12月29日、オバマ大統領は「機密指定された国家安全保障情報(Classified National Security Information)」と題された大統領令13526号（EO13526）を発した[4]。EO13526は、従来の機密指定制度を大きく変更するものであり、現在の米国における機密指定制度の主たる根拠規定となっている。また、オバマ大統領は、EO13526が公布された日に、同命令の施行に関する覚書を発した。その後、情報安全保障監督局（ISOO）は、EO13526の施行規則を、2010年6月25日に公布している[5]。

国家安全保障を維持するためには、連邦政府と州等との情報共有が不可欠である。しかし、連邦制をとる米国では、州やインディアン部族の独立性は高く、連邦政府の機密制度が、そのままこれらの主体に適用されるわけではない。このため、機密保全に関する統一的な扱いに困難が生じる。オバマ大統領は、この問題について、大統領令13549号「州、地方自治体、インディアン部族、及び民間部門における法主体のための機密指定された国家安全保障情報に関するプログラム（Classified National Security lnformation Program for State, Local, Tribal and Private Sector Entities)」[6]を2010年8月に発した。

この1.2条では、この大統領令の目的が、すでに詳述した機密指定制度に関する大統領令13526号と、機密文書等へのアクセスに関する保全基準を定めた複数の大統領令（12968号、13467号、12829号）を、州等に統一的に適用する方策を定めることにあると規定されている。従ってNISP（12829号）も本大統領令により州等に統一的に適用されることとなる。そして、この統一的な実施手続は、この大統領令の公布の日から180日を超えない範囲内で、国土安全保障長官が、実施指令により定めるものとされている。従って実施責任はDoDではなくDHSが担うこととなる。

更にオバマ大統領は、2011年10月に大統領令13587号「機密ネットワークの安全及び機密情報の責任ある共有・防護の改善のための構造改革(Structural Reforms to Improve

[4] http://www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information
[5] http://www.archives.gov/isoo/policy-documents/isoo-implementing-directive.html
[6] http://www.gpo.gov/fdsys/pkg/CFR-2011-title3-vol1/pdf/CFR-2011-title3-vol1-eo13549.pdf

the Security of Classified Networks and the ResponsibleSharing and Safeguarding of Classified Information)」216 を発している。このなかで、特にインサイダー脅威の防止と探知プログラムの実施(2.1 条(b)項)等について規定し第 6 条では「インサイダー脅威に関する特別委員会」について規定している。

NISP は ISOO の指示のもと、権利上はアメリカ合衆国国防長官が執行官となるが、4 つの異なる安全保障機関（Cognizant Security Agencies　CSA）に所轄権を与えている。アメリカ国防総省、アメリカ合衆国エネルギー省、アメリカ国家情報長官（制定時は CIA)、アメリカ合衆国原子力規制委員会 (Nuclear Regulatory Commission) の 4 つで、それぞれに平等の権力がある。そこで国防長官はエネルギー省長官、原子力規制委員会、国家情報長官の同意と影響を受けるすべての機関と協議の上、米国国家産業セキュリティ・プログラム運用マニュアルを（NISPOM）を発行し、維持するための最終的な責任を持つ。

DOD の中では、国防セキュリティサービス（DSS）が、国家産業セキュリティ･プログラムを管理し、国防の部分を実施する。DSS は具体的には、以下のことを行う。

- 国防長官並びに他の 24 の政府機関の長官に代わって NISP の下、約 800,000 の産業関係者のクリリングを実施する
- 機密情報へのアクセスを必要とする請負業者、ライセンスや権限を与えられた人間の点検と監視
- 機密情報を受けることができる施設の保証
- 機密情報を保護するためのオンサイトのセキュリティシステムを保有する請負業者の保証

これに基づき米国国防総省（DOD）は、政府契約企業が政府の機密情報を確実に保全するため、1985 年 3 月に発令した DoD 5220.22-M 機密情報を守るための産業のセキュリティマニュアル（Industrial Security Manual for Safeguarding Classified Information）[7]を改訂し、国家産業セキュリティ･プログラム（NISP：National Industrial Security Program）に基づき、NISPOM として 1995 年 1 月に策定した。本運用マニュアルでは、施設及び人的セキュリティ・クリアランス、情報の機密区分及びマーキング、訪問及びミーティングへの対応等、機密情報保全のための取り組むべき総合的な要件が示されている。

[7] これも NISPOM 同様､防衛産業のセキュリティ･プログラムの中に含まれる契約者に適用されるもので、国防総省の範囲を超えていた。すなわち、それは国防総省のコンポーネントの機密情報を処理する契約者に適用するばかりでなく、18 の他の連邦組織の契約者にも適用する。それらに対して国防長官は、産業のセキュリティサービスをするように行動する権限を与えられていた。18 の他の連邦組織：（注）NASA, 商務省、GSA, State Department, Small Business Administration,科学基金、財務省、運輸省、内務省、農務省、情報局、労働省、環境情報局、司法省、武器管理・武装解除局、連邦危機管理局、連邦予備兵システム、会計検査院

なお、我が国においても、防衛省の装備品の調達に係る契約企業に対しては、契約に基づき秘密保全が義務付けられているが、あくまで防衛秘密等の秘密保護法制の対象企業に限定されるものであり、広く防衛調達企業以外の重要情報を保有する企業を対象としたものではない。

2002 年に制定された連邦情報セキュリティマネジメント法（FISMA：Federal Information SecurityManagement Act、以下、FISMA と称する）[8]は、連邦政府に対し、その情報と情報システムの保護に関する重要な要求事項を定め、米国国立標準技術研究所（NIST：National Institute of Standards andTechnology、以下、NIST と称する）に対しては、連邦政府の FISMA 準拠をサポートするための重要な要求事項を定めている。

こうした重要な法律を踏まえ、NIST は、FISMA 導入プロジェクト[9]の一環として、情報システムセキュリティに関する重要な規格およびガイドラインの策定を行っている。この最重要プロジェクトは、セキュリティ分類規格の策定、情報システムのセキュリティ管理策の仕様、選択、テストに関する規格およびガイドライン、認証のためのレビューおよび情報システムの運用認可についてのガイドライン、そして、意図した通りの運用を確実に行うための継続的な監視についてのガイドラインを含む[10]。特にサイバーセキュリティ関係の技術標準に関しては、NIST では、OMB、NSA、Government Accountability Office（GAO）を始めとする連邦政府機関、および民間企業・団体と協力して策定に当たっている。また、OMB と協力し、技術面から連邦政府機関が FISMA 準拠を達成できるように支援することも NIST の任務の 1 つとなっている。その具体例としては、FIPS や SP 800 シリーズが挙げられる[11]。

3.2.2. NISPOM 要約版

【概要と目次構成】

国家産業保全プログラム（National Industrial Security Program: NISP）は、機密情報を保護するための連邦政府と民間企業との間のパートナーシップであり、その運用マニュアルである NISPOM は、米国政府の請負業者の人員や施設のクリアランスを行い、決定を下すためのガイドラインと範囲を設定する。言い換えれば、NISP / NISPOM は認可施設に

[8] http://csrc.nist.gov/drivers/documents/FISMA-final.pdf
[9] http://csrc.nist.gov/sec-cert/index.html
[10] NIST:THE NEW FISMA STANDARDS AND GUIDELINES CHANGING THE DYNAMIC OF INFORMATION SECURITY FOR THE FEDERAL GOVERNMENT
[11]米国連邦政府のサイバーセキュリティ政策を巡る最近の動向 JETRO 2011 年 3 月

おいてセキュリティ・クリアランスを持つ個人が機密情報のセキュリティを扱うような構成になっている。

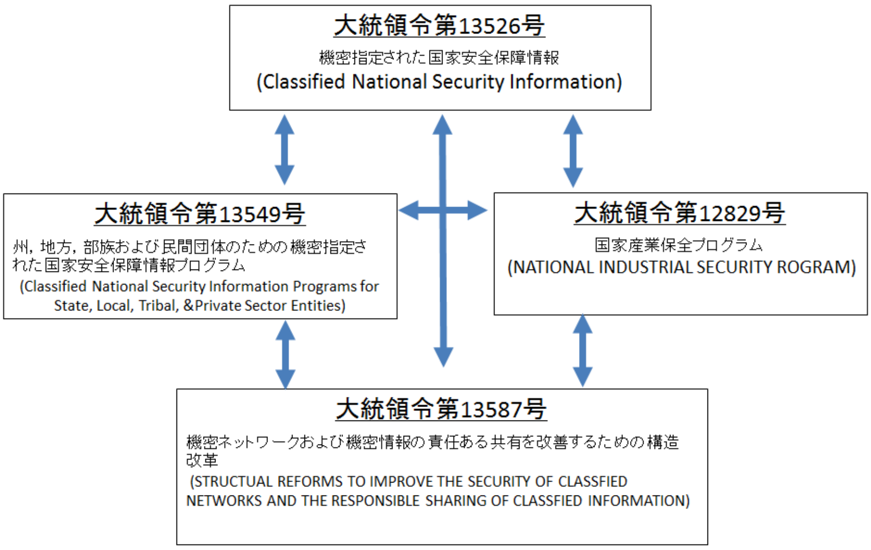
NISPOM は全 11 章から成り、全体を概観する 1 章を除くと 2 章から 7 章までの人的物理的要件と、8 章の IT 要件、9 章から 11 章の特別要件の大きく 3 つに分かれる。また政府組織の重複業務を避ける観点から、互恵契約の原則（reciprocity）（情報システムリソースの再利用や、互いのセキュリティ状態の評価結果を受け入れることによる情報の共有を目的として、参加している組織間で、互いのセキュリティアセスメント結果を受け入れることに合意することをいう）は随所で強調されている（1-207、2-101、2-204）。

目次構成は、次の通りである：

Chapter 1.　総則及び一般的要件
　Section 1.　序説
　Section 2.　一般的要件
　Section 3.　報告に関する要件
Chapter 2.　セキュリティ・クリアランス
　Section 1.　施設クリアランス
　Section 2.　人的クリアランス
　Section 3.　FOCI（外国による所有、管理または影響）
Chapter 3.　セキュリティに関する研修及び概要説明
Chapter 4.　機密区分及び表示
　Section 1.　機密区分
　Section 2.　表記要件
Chapter 5.　機密指定情報の保護
　Section 1.　一般的要求事項
　Section 2.　管理と責任追跡性
　Section 3.　保管と保管装置
　Section 4.　伝送
　Section 5.　開示
　Section 6.　複製
　Section 7.　処分と保有
　Section 8.　構造要求
　Section 9.　不正侵入検知システム
Chapter 6.　立ち入り及び会合
　Section 1.　立ち入り
　Section 2.　会合
Chapter 7.　下請契約
　Section 1.　元請け業者の責任
Chapter 8.　情報システムセキュリティ
　Section 1.　義務及び責任
　Section 2.　評価及び認可
　Section 3.　セキュリティ管理策
Chapter 9.　特別要件

なお NISP と各大統領令の関係は、次の図に示す通りである。

NISPと各大統領令の関係
NISP POLICY RELATIONSHIPS


大統領令第13526号
機密指定された国家安全保障情報
(Classified National Security Information)
大統領令第13549号
州，地方，部族および民間団体のための機密指定された国家安全保障情報プログラム
(Classified National Security Information Programs for State, Local, Tribal, &Private Sector Entities)
大統領令第12829号
国家産業保全プログラム
(NATIONAL INDUSTRIAL SECURITY ROGRAM)
大統領令第13587号
機密ネットワークおよび機密情報の責任ある共有を改善するための構造改革
(STRUCTURAL REFORMS TO IMPROVE THE SECURITY OF CLASSFIED NETWORKS AND THE RESPONSIBLE SHARING OF CLASSFIED INFORMATION)

出展：ISOO Derivative Classification 10-3-12

【各章要約】

Chapter 1. 総則及び一般的要件

○第 1 章の 1-100.で NISPOM が NISP（国家産業保全プログラム）のオペレーションマニュアルであることが述べられる。101 において NISP が大統領令第 13526 号（E.O. 13526）

と原子力法（Atomic Energy Act: AEA）に基づくことと NISP を運用する政府組織体制が述べられる。すなわち、情報保全監督事務所(Information Security Oversight Office: ISOO）長の責任のもと、エネルギー庁長官・原子力規制委員会（Nuclear Regulatory Commission: NRC）議長・国家情報長官（Director of National Intelligence: DNI）長官の同意国防長官が執行する。また管轄保全局（Cognizant Security Agency: CSA）長は CSA 内及び管轄保全事務所（Cognizant Security Offices: CSO）に保全に関わる全側面を権限委譲することが可能となっている。国防長官は産業保全業務を実施する上で各省庁の長官から権限を委譲され代理責任を負う期間協定を結んでいる（103）。また保全管轄権は各省庁が有するがこれの委譲を受けるのが CSA でありその配下の CSO である（104）。201 において請負業者は施設保全適格性確認（Facility Clearance: FCL）の一環として施設保全担当者（Facility Security Officer: FSO）を任命しなければならないとする。206.で請負業者は保全適格性を確認された従業員に、適切で、かつ第 3 章に基づいた保全研修を行うものとしている。

3 節の報告要件においては、最初に情報公開制度上の不開示情報についての判断は CSA が行うとし FCL、人的クリアランス（Personal Clearance: PCL）に影響する事項や秘密情報漏洩についての報告義務（300）や、情報公開法・プライバシー法との関連（300）を述べた後、報告されるべき具体的な PCL に影響する事項（302a-f)、FCL に影響する事項（302g-n)、情報漏洩の報告（303）を述べる。

認可されたすべての請負業者の定期的なセキュリティレビューは、請負業者の安全策が機密情報保護に適切であると確認するため CSA によって行われる。CSA は、このような正式なレビューの頻度も決定するが、通常、審査は毎年実施される。

Chapter 2. セキュリティクリアランス

○施設クリアランス（FCL）（1 節）

請負業者自らが FCL の申請は出来ず、政府側元請け機関（GCA)か、別の認可済みの会社のいずれかによって施設のクリアランスのために保証してもらう(2-102)。CSA は FCL 手続きの間に管理職員の PCL をとり FSO を任命する（103）。FCL でクリアされるためには、いくつかの主要な経営幹部の人的クリアランスをクリアする必要がある（104）。FCL は当事者の一方が終結されるまで有効である（110)。

○人的クリアランス（PCL）（2 節）

FSO はまずアクセスを許可する前に、必ず従業員に機密保持を指示し、従業員と共同で申請手続きを行う（202） TS（機密）（及び Q、SCI）の審査は SF86 電子版を利用して SSBI（Single Scope Background Investigation）で行い、S（極秘）、C（秘）（及び L）の

審査は同じく SF86 電子版を利用して NACLC にて行う。必要に応じポリグラフ検査・財務調査が行われる（201）。

○FOCI（外国による所有、管理または影響 :Foreign Ownership, Control or Influence）（3 節）

FOCI を無効化するためには会社の理事会（Board）あるいは特殊な協定を結び、その中でいくつかの組織・人事的要求がなされる（303）。

Chapter 3. セキュリティに関する研修及び概要説明

第 3 章で 1 節を割いて詳しく研修について述べている。資料が CSA 等から提供されること(3-101)、FSO は 1 年以内に研修を完了すること(102)、内部不正犯行の研修（103)、臨時従業員への教育（105)、初期説明（107)、リフレッシュ教育（108）等が述べられる。

Chapter 4. 機密区分と表示

第 4 章の冒頭で、機密区分は E.O. 13526 の 3 区分即ち TOP SECRET（TS）, SECRET（S）, CONFIDENTIAL（C）であるとし、4-101.の Original Classification.で原機密指定権利者のみが E.O. 13526 の 3 区分を指定できることを明記し、期間についてはまず 10 年、それが難しい場合に最長 25 年まで、それを超える場合は、諸機関間安全保障上訴委員会（The Interagency Security Classification Appeals Panel: ISCAP）の判断によるとしている。原機密を織り込んだり、言い換えたりした派生機密については 102.にてどこまでを派生機密というかを説明し、請負業者が自身の秘密区分マニュアルを作成して適切に指定しなくてはならないとして指定できる条件と指定方法について述べている。

また、書類前面にその機密指定の理由が述べられていることを記載している。105.で請負業者が、機密指定を要する情報を自ら創出し、その情報が機密保全の対象になると判断した場合、当該情報に関する管轄権と機密指定権を有する行政機関に、速やかにその旨を通知する義務を課している。機密指定に対する異議申し立てに関しては 104. Challenges to Classification.でその手順を記載している。

107.では請負業者は契約記載の機密に関するガイダンスもしくは正式書面にて解除、格下げの連絡を受けるとし、たとえ公共のメディアに公開されたからといって、自動的に解除を意味するものでないことを 106.で断っている。原機密指定は原機密指定権利者のみが行えるので機密に関するガイダンスもしくは正式書面にて解除、格下げの連絡を受ける（107)。従って例外・継続などがあったとしても全て正式書面にて通知され請負業者はその指示に

よって行動する。

Top Secret といった標記をどのように行うかについて、例えば文書全体が秘密文書でもその添付資料が秘密でない場合は秘密でないと標記する(205)、グラフが秘密文書に含まれるかどうかも標記する（206）等細部にわたって規定している。

Chapter 5. 機密指定情報の保護

第 5 章が管理の主文であるが、ここでは閉鎖区域(5-306)、保管容器(308)、施錠する鍵(309,310)、入退室管理システム(312,313)、不正侵入検知中央監視所(9 節)等について、その壁、窓、扉、施錠装置、天井、扉、骨組ユニット、その他開口部に至るまでの構造（8 節）が例えば保管庫の場合、壁の厚さは８インチ以上の中空陶製タイル又はコンクリートといったレベル(802b)まで、運用については中央監視所の警備員は PCL が無い場合、警報のあった場所に急行しても PCL を持った要員が駆けつけるまで、もしくは１時間まで現地待機といったレベル(903a(3))まで規定している。更に施設外に持ち出す場合の規定についても利用する輸送業者の指定(402,403,404,405,408,409)はもちろん、運送時は不透明二重包装とし秘密区分や送受信者の記載は内包装表面のみとし、外部から見える表面には宛先住所のみ表記し封印するといったレベル(401a)まで記載している。

同様に開示(5 節)、コピー(6 節)、処分、保有(7 節)についても記載している。防衛関連の活動に伴う機密は防衛関連活動内では他に公開することを認める(505)一方、連邦政府間の機密情報開示は禁じている（506)。

Chapter 6. 立ち入り及び会合

第６章は、機密を扱う施設が訪問を受ける場合の守るべき規則を記載している。

Chapter 7. 下請契約

第７章は、請負業者が下請けを使う場合の規定を行っている。

Chapter 8. 情報システムセキュリティ

情報システムについては８章にまとめられているが、NISPOM の中で最も改変の多い章である。基本は FISMA(Federal Information Security Modernization Act)、NIST(National

Institute of Standards and Technology)800-37、CNSS(Committee on National Security System) 504 等に基づく CSA ガイダンス(8-100)に基づいた自社の ISSP（IS セキュリティプログラム）を制定し(8-101)、セキュリティ計画を策定する（102)。これらは ISSM として任じられた従業員が実施責任を負う(103)。これを評価し認可するのが CSA から指名された権限を持った職員（Authorizing Official: AO）である(2 節)。

機密区分のレベルからの機密性の影響度を判断するのに加え可用性、完全性といった情報セキュリティの要素を織り込んだベースラインを設定し、リスクコントロールを図る（301)。情報セキュリティにおける人的、物理的、環境的保護を実施し、緊急時対応・構成管理を行い運用管理を行う(302)。技術的保護ではアクセス制御、内部監査、ネットワーク境界面保護及び効果的なシステムアーキテクチャ、開発手法、システム工学を使用する（303)。

更に戦術的・組込・DAQ・旧式・特種用途システムについては別途管理策を策定するとし(304)、モバイルシステムについては計画を CSA に連絡するとしている（305)。

情報システムに関するセキュリティ計画を策定しなければならないが（102)、AO の承認があれば情報システムの独自マニュアルも作成可能（304a）である。モバイルシステムについては特別の手順書を作成する必要（304f）がある。情報システムインシデントレスポンスについては 8-101f で簡単に述べられている。

Chapter 9. 特別要件

Restricted Data(RD), Formerly Restricted Data(FRD)、Transclassified Foreign Nuclear Information(TFNI）に指定される核関連情報（1 節および Appendix D)、国防総省重要核兵器設計情報（Critical Nuclear Weapon Design Information: CNWDI）(2 節)、諜報情報（3 節)、通信保全（4 節）についての特別要件を規定している。

Chapter10. 国際的セキュリティ要件

国際的な機密要求については第 10 章にまとまっており AECA（Arms Export Control Act)・EAA（Export Administration Act)・AEA に準拠すること(10-101)、外国権益に対する米国情報の開示（2 節）外国政府情報(3 節) 国際移転(4 節) 国際訪問及び外国人の管理（5 節）(例えば外国人のアクセスがある場合には技術保全計画作成する必要（509）があるなど)、請負業者の海外事業活動(6 節) NATO の情報セキュリティ要件(7 節) 英豪への国防物品移動(8 節)について述べている。

Chapter11. 雑則

請負業者独自の研究開発等に利用する場合は、独自のセキュリティマニュアルを作成する必要（11-302）があるなど。

3.2.3. DoD Information Security Program Manual

2012 年 2 月に Vickers インテリジェンス担当国防次官はそれまでの国防総省における情報セキュリティに関するいくつかの規則に代わり新たに DoD マニュアル 5200.01（DoD Information Security Program: Overview, Classification, and Declassification）を制定した。これにより、従来の４つの DoD 文書（以下）は破棄された。

1. DoD 5200.1-R, Information Security Program, January 14, 1997.
2. DoD O-5200.1-I, Index of Security Classification Guides (U), September 1, 1996.
3. Directive-Type Memorandum 04-010, Interim Information Security Guidance, April 16, 2004.
4. Directive-Type Memorandum 11-004, Immediate Implementation Provisions of Executive Order 13526, Classified National Security Information, April 26, 2011.

DoD マニュアル 5200.01 は複数の部から構成され、それぞれが固有の目的を持っている。国防総省指令（DoDD）5143.01 及び国防総省指導（DoDI）5200.01 で承認されているように、同マニュアル全体の目的は、管理された非機密情報（controlled unclassified information: CUI）及び機密情報の指定、標記、保護並びに配布のための政策の実施、責任の分担並びに手続きの規定を行うことを目的として、国防総省指導（DoDI）5200.01-R を国防総省マニュアルの１つとして再交付することにある。

管理された非機密情報（CUI）及び機密情報には、付随する機微区画情報（sensitive compartmented information: SCI）及び特別アクセスプログラム（Special Access Program: SAP）が含まれる。本指針は DoDI 5200.01-R、大統領令（E.O.）13526 及び大統領令（E.O.）13556 並びに連邦規則集（Code of Federal Regulations）第 32 編 2001 条に従って策定されている。

各巻の内容は以下の通り：

1 巻：
（1）国防総省の情報セキュリティプログラムについて説明

ENCLOSURE2
　関連各職の責務について規定。
　諜報担当国防次官管掌、政策担当国防次官管掌、国防総省 CIO、国防技術情報センター長、ワシントン本部管理局長、国防総省各部局長、公的機関幹部、国防総省現場トップ、現場セキュリティ管理者、機密管理官、公的諜報機関幹部、公的情報システムセキュリティ担当者についてである。

　なお、現場セキュリティ管理者の中で請負業者に対し DoD 5220.22-R の指示に従わせるとあるが、この規制には施設クリアランスや請負業者に対する監査が含まれている。

ENCLOSURE3

項	
1	PURPOSE
2	SCOPE
3	PERSONAL RESPONSIBILITY
4	セキュリティ担当当局の役割について規定。すなわち合衆国大統領（4a で米国大統領が、TS,S,C,CUI の指定権限を有することが規定）、National Security Council (NSC), DNI, ISOO, CUI Office (CUIO)についてである。
5	上記各々の情報セキュリティプログラム管理における役割の詳細
6	
7	請負業者使用時の注意点
8	本マニュアルと EO 13526 が国防総省における原機密指定の根拠であるとの言明
9	国家安全保障の要請によって指定並びに解除される
10	解除後の再機密指定についての規定
11	機密情報へアクセスできる人間のクリアランスについての規定
12	a で RD(Restricted Data)と FRD(Formerly Restricted Data)の、 b で SCI の、c で COMSEC の、d で SAP の、e で NATO と FGI の保護についての規定
13	保有についての規定
14	期限の無い機密についての規定
15	軍事作戦についての規定
16	破棄についての規定
17	不正に対する是正措置と制裁についての規定

18	情報公開法による公開のあとの再機密指定について規定

(2) 国家安全保障のために保護を必要とする国防総省情報の機密指定および機密解除の指針

ENCLOSURE 4

項	
1	機密情報として指定できる類型 (1) 軍事計画､武器システム､又は作戦 (2) 外国政府情報 (3) 諜報活動(秘密活動を含む)、諜報に関する情報源、方法、又は暗号 (4) 機密情報源を含む連邦政府の外交関係又は外交活動 (5) 国家安全保障に関連する科学的、技術的、経済的事項 (6) 核物質又は核施設に対する安全防護策に関する連邦政府プログラム (7) 国家安全保障に関連するシステム、施設、社会基盤、プロジェクト、計画、防護サービスの脆弱性又は能力 (8) 大量破壊兵器の開発､生産､利用に関する情報
2	(a) 機密指定を、①法令違反や過誤の秘匿、②特定の組織等に問題が生じる事態の予防、③競争の制限、④国家安全保障上の利益の保護に必要のない情報の公開を妨げるような目的で行なうことを禁止している。また、このような機密指定を継続したり、機密解除を行わないことも禁じられている。 (b) 国家安全保障上の利益と明白に関係性のない基礎科学研究情報を機密指定してはならないと規定されている。
3	機密情報のレベルは、その重要性に応じて TS,S,C の 3 つの類型に分けられる
4	(a) 原機密は不正に開示されたとき国家安全保障上の損害を予期し特定できる時に初めて指定される (b) 原機密指定者として機密指定できるのは国防長官、各軍長官達と彼らが指定した者 (c) 各機密区分毎の OCA について
5	現機密指定に要請される内容を規定
6	実際の原機密指定の流れが詳細に規定
7	機密区分の変更の手続き
8	機密指定ガイダンスを作ることが規定
9	暫定機密についての規定
10	派生機密の定義や責任、教育など規定

11	派生機密の注意点やなすべきことについての規定
12	派生機密の分類する詳しい手順についての規定
13	有効期間について規定される。まず10年、それが難しい場合に最長25年まで、それを超える場合はthe Interagency Security Classification Appeals Panel（ISCAP　諸機関間安全保障上訴委員会）の判断によることが明記されている他、人的情報源や大量破壊兵器の重要な設計概念が機密の場合、最大75年の期間を指定すること等も規定されている。
14	配布するときの形式について
15	編集した情報（機密とそうでないものがまとめられた情報）についての規定
16	DoDの入手に関する情報について規定
17	情報が公開された後の再機密指定について
18	情報自由化法による公開のあとの再機密指定について
19	機密情報にできない情報
20	機密情報が特許に該当するときには機密特許として分類することを規定
21	機密区分指定の要求がOCA以外からあった場合その要求を受けてから30日以内に判定しなければならない。管轄外のOCAが受けた場合は該当するOCAに照会するとともにその旨を要求者に伝達する。なお、決定が下されるまでは当該情報は保護されなければならない。
22	機密指定に対する異議申し立て

ENCLOSURE 5

DECLASSIFICATION AND CHANGES IN CLASSIFICATION

項	
1	機密指定解除方針 a. EO13526に従う（継続の場合の要件についても） b. OCAとEO13526の規定を満足する上級幹部の判断を要する。 c. 権限無く解除となった機密は管轄OCAとしては機密継続する。（NARA手続きに従って公開されている場合はUSD(I)経由 NARAトップへ提出、25年超の場合ISOOへの提起を含めて） d. 機密解除の表記、あるいは期間延長されていないことを確認して初めて機密解除として利用可能となる e. NARAによる公開以外は機密解除後リリースレビュー無しに機密解除が即ち公開とならない。 f. 退官予定者が解除指示は出来ない。 g. OCAはISCAP決定を機密指定・解除ガイドに反映する

2	解除手続きではEO13526でa.原機密指定権者の決定による解除手続き。b.25年の自動解除手続き。c.請求による義務的機密解除レビュー手続き。d. NARAによるシステム的機密解除審査手続きの4つの解除手続きが規定されていることを述べている。
3	解除権限では、その解除権限のある原機密指定権者について例えば暗号情報についてはNSA / CSSのみが解除・格下げ権限のある事(c)や原機密管轄部門のなくなった場合(d)など細かく規定
4	DECLASSIFICATION GUIDANCE
5	DECLASSIFICATION OF INFORMATION
6	CANCELING OR CHANGING CLASSIFICATION MARKINGS.
7	暗号情報についての手続きを詳細に説明
8	NARAによるシステム的機密解除審査手続きについて20年未満の情報と20年以上の情報との取扱いの違い
9	NARAの保存対象外の機密情報についてはNARA承認のDoD記録管理スケジュールによって解除日に処分する。25年超についてはISCAP承認を受けることを規定
10	25年を超えて機密を継続させる手続き
11	請負事業者所有の機密情報の自動機密解除の注意規定
12	自動機密解除については細かく規定されているが、EO13526でも規定されているとおり①25年での審査、②ISCAP等で機密継続の場合50年か75年で自動解除、③特例（後述の13で規定）による継続機密となるものである。 　12では更に締め切り日の6ヶ月前にUSD（I）への通知の必要性、CUIと指定する場合、RDまたはFRDと記された文書について、期限が複合している場合、レビュー困難な場合の特例としての最大5年の猶予や審査漏れが見つかった場合の90日以内の審査などが規定されている。
13	自動機密解除の例外規定
14	DECLASSIFICATION OF INFORMATION MARKED WITH OLD DECLASSIFICATION INSTRUCTIONS
15	REFERRALS IN THE AUTOMATIC DECLASSIFICATION PROCESS
16	義務的機密解除レビュー：Mandatory Declassification Review（原機密指定を行った行政機関が、機密情報の解除が請求されたときに、その機密情報の解除の適否について審査することをいう（EO13526　6.1条(aa)項で規定されている)。） 　大統領等が作成した情報ではなく当該情報を含んだ資料を合理的な努力によりDoD要員が探し出すことができるように十分に特定して記述されていて、訴訟の対象となっておらず、合衆国法典5編552条(情153報公開法)199における調査、審査、公表、開示から免除されている利用中のファイル(operational file)に含まれておらず（EO13526　3.5条に規定）過去2年以内に機密解除審査がされていない場合（その

	場合はその結果を連絡する）は機密解除審査請求の対象となる。 なお、省内外の別の政府機関による機密指定あるいは影響のある場合は申請者にその旨通知するとともにそれらの組織の決定を収集し最終結果を申請者に連絡する。 また暗号情報は 7 で指定された手続きに従うこと、FGI に関連する場合は条約・国際協定の対象化どうかを調べること、また DoD の諜報セクションに対する要求は米国市民あるいは合法的米国共住外国人以外は拒否される可能性があることなど情報による特別処理があるものの通常、受領日から 1 年以内に最終的な決定を下すとしている。 要請者は、審査の結果受領後 60 日以内であれば機密解除拒絶に対する控訴権を持つ。要求者が上訴を提出した場合、国防総省の上級当局は、受領後 60 営業日以内に決定する。決定を下すために追加の時間が必要な場合、上級当局は、要請された追加の時間を要請者に通知し、延長の理由を提供しなければならない。 不服申し立てが却下された場合、申請者は ISCAP に不服申立てをする権利を通知されるなどが 16 で細かく規定されている。
17	自動機密解除を免除された NARA 指定保存情報について継続的に審査を行うレビュープログラムを作成する
18	格下げについて
19	格上げについて
20	FGI について

ENCLOSURE 6 の SECURITY CLASSIFICATION GUIDES では機密区分の設定ガイドを作ることを要求している

2 巻：機密情報の正しい標記のためのガイダンス
　　機密区分の表記について細かく規定

3 巻：全体が機密情報の保全について規定している
（1）機密情報の保護、保管、破壊、伝達、輸送に関する手引き

ENCLOSURE 2 自体が SAFEGUARDING（安全防護対策）となっており、最初に管理策が策定されなければならずそこには技術的、物理的および人的管理措置が含まれる(1)とし、次に個人の責任(2)、人的クリアランスを経た者のみアクセス出来ること(3)、アクセスの必要性判断(4)、緊急時の特別公開（EO13526 の 4.2 条の b 対応の詳細規定）(5)、さらに部外者への開示については議会やその他の具体的な相手に対して細かく規定（6）し、施設への立入に関しては基本は JPAS による所属とアクセスレベルの確認を行うとしている。（JPAS（Joint Personnel Adjudication System）とは国防総省と請負業者間の人事クリアランスの記録システムのことで、そこには国防総省（DOD）

のすべての活動中のセキュリティ·クリアランスの 90%以上の記録が含まれている。）(7)。

さらに保管場所より取り出した場合の取扱い(8)、日々の確認(9)、テロ・自然災害などの緊急時対応(10)、通信(11)、自宅への持帰り作業(12)、作業文書(13)、機密情報関連機器類(14)、複製(15)、機密に関わる打合・会議（漏洩のリスクが高いとして詳細に規定）(16)、そして（17）では SAFEGUARDING FGI として外国政府関連情報の安全対策を詳述している。最後に(18)で標準規定では Need To Know が満足させることができない時にとる代替措置（ACCM）についての規定で SAFEGUARDING（安全防護対策）を閉じている。

そして 2 章に当たる ENCLOSURE 3 では保管について、3 章に当たる ENCLOSURE 4 では通信と移送について各々1 章をあてている。また設備の物理的規格などは付録で詳細に規定している。

（2）セキュリティ違反や機密浸食に対する処理の要件と手順についてのセキュリティ教育とトレーニング

ENCLOSURE 5 が SECURITY EDUCATION AND TRAINING である。

ENCLOSURE 6 でセキュリティインシデント（SECURITY INCIDENTS INVOLVING CLASSIFIED INFORMATION）を取り扱っている。

（3）セキュリティ管理者が認識しなければならない情報技術（IT）の問題

ENCLOSURE 7 が IT ISSUES FOR THE SECURITY MANAGER となっており、IT 関連の規定となっている

4 巻：CUI の識別と保護の指針

ENCLOSURE 2: RESPONSIBILITIES は USD(I)をはじめとする各部局の役割について規定している

ENCLOSURE 3: IDENTIFICATION AND PROTECTION OF CUI

1. GENERAL.

CUI として指定してはいけないものとして EO13526 の 1.7 条(a)同様に①法令違反、非効率性の助長、又は行政上の過誤の秘匿、②特定の個人、組織、又は行政機関に問題が生じる事態の予防、③競争の制限、又は、④保護に必要のない情報の公開を妨げ、又は遅延させる目的で行なうことを禁止し(a)、逆に本来の機密区分に該当するものや CUI とするのに重大な疑義のあるものも禁止(b)、また一般

に公開された情報を CUI とできない(c)ことを規定している
(d)で書類作成者が指定できるが、権限のあるものが変更することを妨げない ことを規定している。
(e)で請負業者に CUI 情報を提示する時の規定を定めており(f)(g)で CUI 情報の外国政府への開示についての規定がある、(h)で輸出規制との関係について、
(i)では任務遂行上の開示について定め、(j)ではセキュリティ分類ガイドあるいはその解除後は別途覚書か同様のガイドでガイダンスすることを規定している
(k)において CUI の不正な開示について言及されている
(l)で処分について、(m)で例外について触れている

2 以下 6 まででは個々の CUI について取扱いを規定している。

2. FOUO INFORMATION
   情報公開制度上の不開示情報
3. LES INFORMATION
4. DoD UCNI
5. IMITED DISTRIBUTION INFORMATION
6. OTHER AUTHORIZED DESIGNATIONS
   DoS SBU, DEA Sensitive information についてまとめている
7. FOREIGN GOVERNMENT INFORMATION として 1 項を設けている。
8. DISTRIBUTION STATEMENTS ON TECHNICAL DOCUMENTS
   では技術文書の配布についての規定が述べられている。

ENCLOSURE 4 では CUI EDUCATION AND TRAINING として 1 項が設けられている

4.　我が国の技術情報保全の在り方の方向性

企業等の情報保全の在り方に関して、仕様書に示す以下の観点を分析軸とし、次ページの表に整理した。

○組織体制（人事体制等）
○情報保全マニュアルの作成
○秘密情報区分及びその判断主体、判断基準
○秘密情報にアクセス可能な人員のクリアランス
○秘密情報を保管する施設のクリアランス
○認証、定期的なモニタリング監査
○不正に対する対応

3 回にわたる委員会での議論および企業や関係者へのヒアリングを通して得た大きな結論として、「我が国の重要技術情報を守り育てるためには何らかのガイドラインが必要」という点を挙げることができる。

また、そのガイドラインが米国を始めとする他国のガイドラインと比較して、どのような位置づけになるかは、下記比較表に示す現況の参考等と今後整備されるガイドラインを踏まえての今後の検討課題となるだろう。

検討の際には、検討委員会の意見から下記の観点が加味されるよう提案したい。

① 国家安全保障上の『重要技術』と企業にとっての意味を対応づけて対策を検討すべきではないか。
② 防衛省の『保護情報』対策でも企業は苦労しているという実態があり、今後進められる重要技術の保全に関しては企業側のインセンティブを検討すべきではないか。
③ 政府機関と企業での保護レベルを整合すべきではないか（企業秘密の政府機関での取扱規定等）。
④ 保護施策と情報共有施策はバランスを取って同時に実施しないと、企業競争力・活力が失われるため、今回の施策に対応する情報共有施策も必要ではないか。
⑤ 米国とセキュリティ対策で日本と齟齬がある点は、米国は個人が責任をとり、日本は組織（職制上の立場）が責任をとるという点であり、充分な検討が必要ではないか。

【日米の情報保全制度の比較】

分析軸		米国	日本		米国 NISPOM と日本との相違点
		NISPOM	秘密情報の保護ハンドブック	ISMS* JISQ27002	
1.	組織体制（人事体制等）	▲1-101,1-104. 1-201.2-303.	○ ４章	▲ 6.1.1	ハンドブック：日本の企業の実情をベースに管理体制を記述しているので日本企業の各部門がどう協力して管理するかを書いており詳しい。 ISMS：国際標準であり抽象的な記述。 NISPOM：国として重要な秘密をどう企業に守らせるかの視点。 責任者としての FSO の設置とトップの関与などを規定する。
2.	組織が情報保全マニュアルを作成する必要有無及びマニュアルの項目	○1-100, 4-102. 8-102, 8-304a, 8-304f, 10-509, 11-302,11-303	○ 3－3 ４－１	○ 5.1.1、 12.1.1,	日本２例：社内での秘密保全規則を作り守るガイドの役割 NISPOM：国として守らせるべき規制で、基本はこのマニュアル通りに運用することがベース。その中で IT セキュリティ計画や自社研究での使用手順などを作らせることも規定している。
3.	機密情報の指定と解除等	４章			日本２例：自社の秘密を守ることのガイド ➡何を秘密とすべきかどう分類するかは重点項目となる 有効期間や緩和措置は非公知性が失われた時点という程度になる。 NISPOM：国で決められた秘密を守らせるマニュアル ➡どう決められているかは大統領令などで規定。 それを受けて適合事業者が新たに秘密となるものを作り出した時（派生機密）については細かく規定。 公共のメディアに公開されたからといって自動的に解除を意味するものでなく、契約記載の機密に関するガイダンスもしくは正式書面にて解除、格下げの連絡を受けるまでは緩和措置を取らないようにクギを指している。 また国の持つ秘密であるため国民への開示の関係から情報公開制度との関係や秘密の有効期間への言及がある。 情報公開制度上の不開示情報についての判断は CSA が行うとされている
	3.1. 原機密指定と機密情報の対象範囲	○ 4-101 （EO13526）、	○ ２－１ ２－２	○ 8.1.1	
	3.2. 機密情報の区分とその判断主体（原機密指定権を有する者）	○4-101 （EO13526）、 4-102 4-105	▲ ３－１	○ 8.2.1, 8.2.2	
	3.3. 有効期間（初期・延長）	○4-101	×	▲8.2.1	
	3.4. 判断基準・要件	▲4-101 4-104	２－２（１）	▲8.2.1	
	3.5. （機密指定の）緩和措置				
	3.5.1 機密指定解除（Declassification）、機密指定の格下げ（Downgrading）	○ 4-107 4-106	×	▲ 8.2.1	
	3.5.2. （自動機密解除に対する）機密解除の例外、機密指定の継続	▲ 4-107	×	×	
	3.6. 情報公開制度上の不開示情報（情報公開法の適用除外情報）	▲ 1-300b	×	×	
4.	機密情報の保全関連				NISPOM：機密を守らせる立場から適格性を判断し認可するクリアランスは重要で詳細に規定している。 FSO はまずアクセスを許可する前に、必ず従業員に機密保持を指示し、従業員と共同で申請手続きを行う。請負業者自らが FCL の申請は出来なく、政府側元請機関か別の認可済みの会社のいずれかによって施設のクリアランスのために保証してもらう 日本２例：自分に認可を与えてもあまり意味がない ハンドブック：取引先に営業秘密を扱う資格審査 ISMS:サテライトオフィス・供給者としての資格審査
	4.1.人クリアランス（有の場合には、その区分、調査事項と方法、有効期限等）	○ 2-2	×	×	
	4.2.施設クリアランス有の場合には、その区分、調査事項と方法、有効期限等）	○ 2-1	▲ ３－４（３）	▲ 6.2.2, 15	
	4.3.監査又は認証（有の場合には、その方法）	○ 1-207	▲３－４（１）p ３－４（２）a	▲ 12.7, 15.2.1	実際の機密保全措置は保全の主項目、どの規定も詳細に記載している 日本２例：自社の秘密を守る推奨表現。 NISPOM：守らせる規制表現。かなり詳細な規定、以下にレベルの例 保管庫：壁の厚さは８インチ以上の中空陶製タイル又はコンクリート 中央監視所の警備員：人的クリアランスの無い場合警報のあった場所に急行してもクリアランスを持った要員が駆けつけるまで、もしくは１時間まで現地待機
	4.4.機密情報の管理（人・施設）	○ 4.2、5,6,7	○ 3－2 3－4	○ 6, 7, 8.1.2 8.1.3、8.1.4 8.2.3, 8.3, 11	
	4.5.情報セキュリティ	○8 章	▲３－４（１）（３）	○（全体）6.2.1 9,10,12,13,14	
5.	不正に対する対応（罰則や報告等）	○1-3、8-101f	○6章	○7.2.3, 16	
6.	他組織（又は国）との相互認証	○1-103, 1-104, 1-207, 2-101, 2-204, 5-505, 5-506、10 章	×	▲ 6.1.3, 6.1.4, 18	NISPOM：NATO その他外国情報を取り扱う場合などの規定 ISMS：コンプライアンス及び関連組織との連携についての記述。
7.	人材育成の仕組み（情報保全のモニタリング要員等）	○3 章, 1-206	○ ３－４（１）④a ３－４（４）d	○7.2.2	NISPOM：３章全体があてられ資料が CSA 等から提供されること(3-101)FSO は１年以内に研修を完了すること(3-102)内部不正の研修（3-103）臨時従業員への教育（3-105）初期説明（3-107）リフレッシュ教育（3-108）等が述べられる。
8.	その他特徴的な部分		自社秘密防衛教育本。加害者にならない対策も詳述	政府下請限定ではないが、内容項目は NISPOM に近い	

*ISMS＝情報システムマネジメント標準

○：言及あり　▲：言及はあるが観点が異なる／不十分等　×：言及無し

巻末参考資料

参考資料①～③では、DoD の産業保全に関する文書を対象に以下の項目に該当する部分を抜粋し掲載している。

- 組織体制（人事体制等）
- 組織が情報保全マニュアルを作成する必要有無及びマニュアルの項目
- 機密情報の指定と解除等
- 機密情報の保全関連
  - 施設クリアランス
  - 監査又は認証
- 不正に対する対応（罰則や報告等）
- 他組織との相互認証
- 人材育成の仕組み

参考資料④は、DoD マニュアル 5200.01. (vol.2)に規定される「マーキング原則 (Marking principles)」を抜粋したものである。

参考資料⑤は、NIST による ISO/ICE27001 の比較である。

① DoDI NUMBER 5200.01

DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)

EO13526に伴う、SAP、SCI、CUIに関するポリシーと各部署の責任を命じたものである

1. PURPOSE. In accordance with the authority in DoD Directive (DoDD) 5143.01 (Reference (a)), this instruction:

a. Reissues DoD Instruction (DoDI) 5200.01 (Reference (b)) to update policy and responsibilities for collateral, special access program, SCI, and controlled unclassified information (CUI) within an overarching DoD Information Security Program pursuant to Executive Order 13526; part 2001 of Title 32, Code of Federal Regulations; section 3038(a) of Title 50, United States Code; DoDD 5205.07; and Executive Order 13556 (References (c) through (g), respectively).

b. Establishes policy and assigns responsibilities regarding the protection, use, and dissemination of SCI within the DoD pursuant to References (a), (c), and (e) and Executive Order 12333 (Reference (h)).

1.1. 組織体制（人事体制等）

ENCLOSURE 2. RESPONSIBILITIES.で SAP、SCI、CUIに関するポリシーと各部署の責任を命じている

ENCLOSURE 2
RESPONSIBILITIES

l. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)). As the senior security official and the senior agency official responsible for the DoD Information Security Program in accordance with References (a) and (c), the USD(I):

a. Develops, coordinates, and oversees the implementation of a DoD Information Security Program that encompasses CUI, SCI, special access programs, and collateral information and activities.

b. Develops information security policy and guidance and oversees DoD implementation of References (c) and (g), Executive Order 13549 (Reference (u)), and the DoD Information Security Program.

c. Consults, as necessary, with other Principal Staff Assistants when developing information security policy directly affecting their areas of assigned responsibilities.

d. Approves, as necessary, requests for exceptions and waivers to DoD Information Security Program policies and procedures except for those involving the responsibilities of the Under Secretary of Defense for Policy for programs listed in paragraph 7a of this enclosure and the responsibilities of the Military Departments listed in paragraph 12 of this enclosure.

e. Directs, administers, and oversees the disclosure of classified military information in category 8 (military intelligence) to foreign governments and international organizations, and coordinates with the Under Secretary of Defense for Policy on the portions of the DoD Information Security Program listed in paragraph 7a of this enclosure, including exemptions and waivers thereto.

f. In coordination with the Under Secretary of Defense for Acquisition, Technology, and Logistics and the DNI, supports research to assist the NDC in addressing the cross-agency challenges associated with declassification.

g. Coordinates with the Chief Information Officer of the Department of Defense to develop policies, including those for information assurance, that provide for the security of information in a networked environment.

2. DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA). Under the authority, direction, and control of the USD(I), in addition to the responsibilities in section 11 of this enclosure, and in accordance with References (a), (c), and DoDD 5105.21 (Reference (v)), the Director, Defense Intelligence Agency:

a. Maintains Reference (n).

b. Administers DoD SCI security policies and procedures issued by the DNI, except with respect to the National Security Agency/Central Security Service (NSA/CSS), National Reconnaissance Office (NRO), and National Geospatial-Intelligence Agency (NGA). At a minimum, the Director, DIA:

(1) Incorporates within Reference (n) SCI security policies and procedures issued by the DNI, and all DNI-issued changes or modifications thereto.

(2) Inspects and accredits DoD and DoD contractor facilities for the handling, processing, storage, and discussion of SCI.

(3) Inspects accredited DoD and DoD contractor SCI facilities on a recurring basis to determine continued compliance with established SCI security policies and procedures.

(a) Issues reports detailing any deficiencies noted and corrective action required.

(b) When appropriate, shares information of mutual interest with the Directors of the Defense Security Service and Defense Contract Management Agency.

(4) As required or directed by the DNI or the USD(I), gathers data and prepares and submits reports to the DNI through the USD(I), regarding the status of implementation of SCI security policies and procedures within the DoD.

(5) Monitors the establishment and maintenance of SCI security awareness, education, and certification programs within the DoD Components in accordance with DoDI 3305.13 and DoD 3305.13-M (References (w) and (x)).

(6) Develops and coordinates recommendations on current and proposed DNI SCI security policy and procedures with the senior intelligence officials designated in accordance with References (i) and (n).

(7) On behalf of the DoD Components and their subordinate elements, establishes memorandums of agreement with NSA/CSS, NRO, and NGA and non-DoD federal agencies for joint use of SCI-accredited facilities.

(8) Operates SCI security programs to support other DoD activities and federal agencies by special agreement, in accordance with Reference (n).

3. DIRECTOR, NSA/CHIEF, CSS (DIRNSA/CHCSS). Under the authority, direction, and control of the USD(I), in addition to the responsibilities in sections 6 and 11 of this enclosure and in accordance with References (a), (c), and DoDD 5100.20 (Reference (y)), the DIRNSA/CHCSS:

a. As the designee of the Secretary of Defense, when necessary, imposes special requirements on the classification, declassification, marking, reproduction, distribution, accounting, and protection of and access to classified cryptologic information.

b. Develops implementing guidance, as necessary, for the protection of signals intelligence.

4. DIRECTOR, NGA. Under the authority, direction, and control of the USD(I), in addition to the responsibilities in sections 6 and 11 of this enclosure and in accordance with References (a), (c), and DoDD 5105.60 (Reference (z)), the Director, NGA develops implementing guidance, as necessary, for the protection of imagery, imagery intelligence, and geospatial information.

5. DIRECTOR, NRO. Under the authority, direction, and control of the USD(I), in addition to the responsibilities in sections 6 and 11 of this enclosure and in accordance with References (a), (c), and DoDD 5105.23 (Reference (aa)), the Director, NRO develops implementing guidance, as necessary, for the protecting information related to research and development (R&D), acquisition, launch, deployment, and operation of overhead reconnaissance systems, and related data-processing facilities to collect intelligence and information to support national and DoD missions and other United States Government (USG) needs.

6. DIRNSA/CHCSS AND DIRECTORS, NRO AND NGA. Under the authority, direction and control of the USD(I), the DIRNSA/CHCSS and Directors of the NRO and NGA establish, direct, and administer all aspects of their respective organization's SCI security programs, to include all necessary coordination and implementation of DNI security policy, consistent with Reference (a) and applicable authorities as heads of elements of the IC in accordance with Reference (h).

7. UNDER SECRETARY OF DEFENSE FOR POLICY. The Under Secretary of Defense for Policy:

a. Directs, administers, and oversees those portions of the DoD Information Security Program pertaining to foreign government (including the North Atlantic Treaty Organization) classified information; the disclosure of classified military information in categories 1 through 7 to foreign governments and international organizations, consistent with DoDD 5230.11 (Reference (ab)); and security arrangements for international programs, consistent with DoDD 5111.1 (Reference (ac)) and other relevant policies.

b. Coordinates those portions of the DoD Information Security Program listed in paragraphs 1d and e of this enclosure, including exemptions and waivers thereto, with the USD(I).

c. Approves requests for exception or waiver to policy involving any policy or programs listed in paragraphs 1.d and 1.e of this enclosure.

8. UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS. In accordance with Presidential Memorandum (Reference (ad)), in coordination with the DNI and the USD(I), the Under Secretary of Defense for Acquisition, Technology, and

Logistics supports research to assist the NDC in addressing the cross-agency challenges associated with declassification.

9. CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF DEFENSE. The Chief Information Officer of the Department of Defense coordinates with the USD(I) when developing policies, including those for information assurance, that provide for the security of information in a networked environment and are consistent with the requirements of References (i) and (n), DoD 5200.2-R (Reference (ae)), and other guidance issued by the USD(I) and the DNI.

10. DIRECTOR, WASHINGTON HEADQUARTERS SERVICE. Under the authority, direction, and control of the Department of Defense Deputy Chief Management Officer (DCMO), in addition to the responsibilities in section 11 of this enclosure and in accordance with References (a), (c), and DoDD 5110.04 (Reference (af)), the Director, Washington Headquarters Service, develops implementing guidance, as necessary, for the protection of information related to providing a broad range of administrative, management, and common support services, including human resources and security clearance services, facilities and facility operations, information technology (IT) capabilities and services, financial management, acquisition and contracting, and secure communications while also providing oversight of designated DoD-wide statutory and regulatory programs, supporting DoD Components and other federal entities as directed and assigned.

a. Directs and administers a DoD Mandatory Declassification Review Program in accordance with DoD 5230.30-M (Reference (ag) and consistent with subsection 3.5 of Reference (c), to include establishing:

(1) Procedures for processing mandatory declassification review requests and appeals consistent with subsection 3.5 of Reference (c), section 2001.33 of Reference (d), and Reference (i). Procedures will ensure that requests for review of documents issued by the Inspector General of the Department of Defense are forwarded to the office of the Inspector General for processing.
(2) A database to facilitate consistency of reviews and declassification decisions.

b. Directs and administers the OSD Automatic Declassification and Review Program consistent with subsection 3.3 of Reference (c).
c. Provides for the security review of DoD information, consistent with the requirements of Reference (o), including establishing procedures for:

(1) Processing security review requests, including appeals, in accordance with References (p) and (q).
(2) Clearing of material subject to parts 120-130 of Title 22, Code of Federal Regulations and section 2751 of Title 22, United States Code (References (ah) and (ai)).
(3) Processing Department of State "Foreign Relations of the United States" documents, including appeals, consistent with Foreign Relations of the United States Program requirements (i.e., section 4353 of Reference (ai)).

11. DOD COMPONENT HEADS. The DoD Component heads:

a. Protect classified information and CUI from unauthorized disclosure consistent with References (c) and (i).
b. Designate a senior agency official to be responsible for the direction, administration, and oversight of the DoD Component's information security program, to include:

(1) Classification, declassification, and safeguarding classified information.
(2) Security education and training programs.
(3) Implementation of References (c) and (i).

c. DoD Component heads who lead IC components in accordance with Reference (h) will appoint the senior intelligence official to oversee their SCI program.

d. Ensure the senior agency official and the senior intelligence official coordinate to achieve a cohesive information security program.

e. Provide adequate funding and resources to implement classification, declassification, safeguarding, oversight, and security education and training programs.

f. Establish and maintain an ongoing self-inspection program to include periodic review and assessment of the DoD Component's classified information and CUI products.

g. Direct and administer a program for systematic declassification reviews as required by subsection 3.4 of Reference (c), to declassify records as soon as possible, but not prematurely, and for review of information subject to the automatic declassification provisions of subsection 3.3 of Reference (c).

h. Establish and maintain an active security education and training program to inform personnel of their responsibilities for protecting classified information and CUI.

(1) Train all original classification authorities and derivative classifiers in the fundamentals of security classification, the limitations of their authority, and their duties and responsibilities as a prerequisite to exercising this authority.

(2) Train all personnel to provide a basic understanding of the nature of classified information and CUI and the proper protection of such information in their possession to include responsibilities for the protection of classified information and CUI from unauthorized disclosure.

(3) Incorporate security education and training, as appropriate, into DoD contracts.

(4) Brief onsite support contractor personnel in security responsibilities, procedures, and duties applicable to their positions.

i. Submit DoD information intended for public release for review in accordance with paragraph 3.k of this Instruction.

j. Establish a system for the receipt of and action on complaints and suggestions regarding the DoD Component's information security program.

k. Forward recommendations for improvements to the DoD Information Security Program to the USD(I)'s Director for Defense Intelligence (Intelligence & Security)/Security Policy and Oversight Division.

l. Participate in the NDC by providing:

(1) The necessary resources to process declassification referrals containing DoD Component information under the purview of the NDC and in accordance with the NDC processing standards.

(2) Training to declassification reviewers in accordance with NDC training standards.

(3) Declassification reviews in accordance with the quality standards of the NDC.

(4) Initial reviews of records eligible for automatic declassification in accordance with Reference (i) and the priorities and implementing instructions issued by the NDC in accordance with References (c) and (d).

m. Ensure that classified information and CUI are managed and retained in accordance with DoD Component authorized records management manuals and schedules, as approved by the National Archives and Records Administration in accordance with Chapters 31 and 33 of Title 44, United States Code (Reference (aj)) and Public Law 113-187 (Reference (ak)).

12. SECRETARIES OF THE MILITARY DEPARTMENTS. In addition to the responsibilities in section 11 of this enclosure, the Secretaries of the Military Departments:

a. As agency heads and designated senior agency officials as defined by and in accordance with Reference (c), in cooperation with the USD(I), participate in the development and coordination of applicable Executive orders, security policy directives, and related issuances.

b. Develop and coordinate the Military Department information security policy and guidance, and oversee the Military Department implementation of References (c), (d), (i), (t) and the Military Department's Information Security Program.

c. Approve, as necessary, requests for exceptions and waivers to the Military Department's Information Security Program policies and procedures identified in paragraphs 10a and 10b of this enclosure except for those involving the responsibilities of the Under Secretary of Defense for Policy for programs listed in paragraph 7a.

13. CHAIRMAN OF THE JOINT CHIEFS OF STAFF. In addition to the responsibilities in section 11 of this enclosure, the Chairman of the Joint Chiefs of Staff provides oversight of the Combatant Commands' information security programs.

1.2.　組織が情報保全マニュアルを作成する必要有無及びマニュアルの項目

3.POLICY の i では DoD 情報セキュリティプログラムポリシーが DoDD 5200.43 に従って開発されるとしている。

i. DoD Information Security Program policies will be developed to standardize processes and best practices in coordination with the Defense Security Enterprise pursuant to DoDD 5200.43 (Reference (m)).

1.3.　機密情報の指定と解除等

○判断基準・要件

3. POLICY の c で EO13526 同様①法令違反や過誤の秘匿、②特定の組織等に問題が生じる事態の予防、③競争の制限、④国家安全保障上の利益の保護に必要のない情報の公開を妨げるような目的で行なうことを禁止している。

c. Information will not be classified, continue to be maintained as classified, or fail to be declassified, or be designated CUI under any circumstances in order to:

(1) Conceal violations of law, inefficiency, or administrative error.

(2) Prevent embarrassment to a person, organization, or agency.

(3) Restrain competition.

(4) Prevent or delay the release of information that does not require protection in the interests of national security or as required by statute or regulation.

○（機密指定の）緩和措置

・機密指定解除（Declassification）、機密指定の格下げ（Downgrading）

3.POLICY の b で必要期間が過ぎれば解除を、l で NDC の設定した機密解除ガイドラインに則ることをポリシーとすると述べる。

b. Declassification of information will receive equal attention as the classification of information so that information remains classified only as long as required by national security considerations.

l. In accordance with the provisions of section 3.7 of Reference (c), DoD will comply with guidelines set by the National Declassification Center (NDC) within the National Archives for streamlining declassification processes, facilitating quality assurance measures, and implementing standardized training regarding the declassification of records determined to have permanent historical value.

・（自動機密解除に対する）機密解除の例外、機密指定の継続

3. POLICY の k で一般公開前のレビューについて言及している。

k. Before being approved for public release, all DoD information will be reviewed pursuant to Reference (i); DoDD 5230.09, DoDI 5400.04, DoDI 5230.29, and DoDI 8550.01 (References (o) through (r), respectively); and other applicable policies including, but not limited to DoDD 5122.05 (Reference (s)).

○情報公開制度上の不開示情報（情報公開法の適用除外情報）

.

1.4.　機密情報の保全関連

○機密情報の管理（人・施設）

3. POLICY の d では機密情報及び CUI の量を最小限にすること、e 情報共有を促進し管理の簡素化を図ること、f..SCI に関しては DNI によって確立された方針と手順に従って保護、g.機密情報は DoDI 5220.22 によって保護する、j で 5105.21 に従って、機密情報と CUI を不正な開示から保護することをポリシーとしている

d. The volume of classified national security information and CUI, in whatever format or media, will be reduced to the minimum necessary to meet operational requirements.

e. The DoD Information Security Program will harmonize and align processes to the maximum extent possible to promote information sharing, facilitate judicious use of scarce resources, and simplify its management and implementation.

f. SCI will be safeguarded in accordance with policies and procedures established by the DNI.

g. Classified information released to industry will be safeguarded in accordance with DoDI 5220.22 (Reference (j)).

j. Security requirements and responsibilities for protecting classified information and CUI from unauthorized disclosure will be emphasized in DoD Component training programs, pursuant to References (c), (d), and (i), and DoD Manual 5105.21 (Reference (n)).

1.6. 不正に対する対応（罰則や報告等）

3. POLICY の h では内部不正、セキュリティインシデントへの対応の準拠資料を提示、m で機密情報の故意、過失、および意図せぬ誤った取り扱いに対処する保護要件およびインシデント対応策は、“Unauthorized Disclosures of Classified Information or Controlled Unclassified Information on DoD Systems,”に従って実施されなければならない。としている。

h. DoD Information Security Program policies, assigned responsibilities, and best practices will be developed to counter, manage, and mitigate the insider threat pursuant to DoDD 5205.16 (Reference (k)) and serious security incidents involving classified information in accordance with Reference (i) and DoDD 5210.50 (Reference (l)).

m. Safeguarding requirements and incident response measures addressing willful, negligent, and inadvertent mishandling of classified information must be implemented across DoD in accordance with Deputy Secretary of Defense Memorandum (Reference (t)). Commanders and supervisors at all levels must consider and, at their discretion, take appropriate administrative, judicial, contractual, or other corrective/disciplinary action to address negligent discharges of classified information commensurate with the seriousness of the security violation.

② DoD Manual Number 5205.07

Volume 1: DOD Special Access Program (SAP) Security Manual

General Procedures

This manual is composed of several volumes, each containing its own purpose. The purpose of the overall manual, in accordance with the authority in DoD Directive (DoDD) 5143.01 (Reference (a)), is to implement policy established in DoDD 5205.07 (Reference (b)), assign responsibilities, and provide security procedures for DoD SAP information.

1.1 組織体制（人事体制等）

○政府側で SAP を管理する GPM、その実行を管理する PSO、請負業者側で実行を管理する CPM、CPM に任命される請負業者のプログラムセキュリティ責任者 CPSO とその間のコーディネートを行う政府の GSSO、そして TS SAP の資料に対するアクセス、責任、および在庫記録の受領、発送、送信、および保守を担当する TSCO の各役割について ENCLOSURE 3 で述べる。

ENCLOSURE 3：FUNCTIONAL ROLES

1. GOVERNMENT PROGRAM MANAGER (GPM). The GPM:

a. Manages designated SAPs.

b. Implements and executes SAP security countermeasures in accordance with all applicable laws; national, DoD, and DoD Component issuances relating to or governing DoD SAPs; and this volume.

c. Monitors and assigns personnel, financial resources, and facilities required to establish, support, and maintain SAPs and security compliance.

d. Implements operations security (OPSEC), treaty, and arms control measures needed to support the SAP and ensure a tailored Security Education and Training Awareness (SETA) program for all briefed personnel.

e. Plans and budgets for program cybersecurity resources, ensuring compliance with established cybersecurity policy for all systems, including those under contract or vendorprovided.

f. Complies with applicable cybersecurity and technology acquisition requirements in accordance with DoDD 5000.01 (Reference (i)) and Interim DoDI 5000.02 (Reference (j)) for all IS acquisitions.

g. Serves as the IS Owner in accordance with the DoD Joint Special Access Program Implementation Guide (Reference (k)).

2. PSO. The PSO, appointed by the CA SAPCO, is responsible for the program security management and execution of all security policies and requirements for a specific SAP(s) program(s), compartment(s), sub-compartment(s), or project(s), and:

a. Works with the GPM to develop, implement, and enforce a security program that protects all facets of the SAP. Provides security subject matter expertise to the GPM and oversight to assigned programs to ensure compliance with all established policy and procedures.

b. Provides oversight and direction for SETA programs.

c. Provides oversight and direction to government SAP security officers (GSSOs) and contractor program security officers (CPSOs) designated to support SAPs.

d. Conducts or verifies that all approved SAPFs are properly inspected for security compliance.

e. In coordination with the appropriate government CI activity, applies risk management principles to SAP security architectures and environments for which the PSO is responsible. These principles include but are not limited to:

(1) Identify, characterize, and assess threats.

(2) Assess the vulnerability of critical assets to specific threats.

(3) Determine the risk (i.e., the expected likelihood and consequences of specific types of attacks on specific assets).

(4) Identify ways to mitigate those risks.

(5) Identify and assess cost and resources to mitigate those risks.

(6) Prioritize risk mitigation measures based on a strategy.

f. Approves changes to the environment and operational needs that could affect the security authorization in accordance with Reference (k).

g. Verifies that configuration management policies and procedures for authorizing the use of hardware and software on an IS are followed in accordance with Reference (k).

h. Ensures that each assigned GSSO and CPSO conducts and documents annual selfinspection. Approves the resultant corrective actions to establish or ensure compliance.

i. Ensures that a SAP trained and knowledgeable GSSO or CPSO, as appropriate, is assigned to serve as the SAP security official at each organization or facility.

j. Initiates and directs security investigations and inquiries to fully explore and document security incidents.

3. GSSOs and CPSOs. GSSOs and CPSOs:

a. Coordinate with the PSO and the GPM or Contractor Program Manager (CPM), respectively, to create a secure environment to facilitate the successful development and execution of a SAP(s) at each organization or location where SAP information is stored, accessed, or SAP-accessed personnel are assigned.

b. Are responsible for security management, to include SETA, and operations within their assigned activity, organization, or office.

c. Adhere to applicable laws as well as national, DoD, and other security SAP policies and requirements.

d. Coordinate SAP security matters with the PSO and GPM or CPM, respectively.

e. Establish, conduct, and document initial, event-driven, and annual refresher training for all assigned SAP-accessed individuals.

f. Conduct an annual self-inspection, document the self-inspection, and submit to the PSO a corrective action plan that identifies actions to establish compliance.

4. CPM. CPMs will:

a. Assign in writing a CPSO to serve as the SAP security official at each contractor organization or location where SAP information is stored or accessed or SAP-accessed personnel are assigned.

b. Be responsible for execution for the statement of work, contract, task orders, and all other contractual obligations.

5. TOP SECRET (TS) CONTROL OFFICER (TSCO). TSCOs will be responsible for the receipt, dispatch, transmission, and maintenance of access, accountability, and inventory records for TS SAP material. TSCOs will be designated in writing by the GPM or CPM, when the PSO determines a program requires a TSCO. The processes used by the TSCO will be thoroughly documented in the standard operating procedures (SOPs).

1.2.　組織が情報保全マニュアルを作成する必要有無及びマニュアルの項目

○PROGRAM PROTECTION PLAN を作ることが規定されている。

ENCLOSURE 4
GENERAL PROVISIONS AND REQUIREMENTS

6. PROGRAM PROTECTION PLAN (PPP). All SAPs will develop, implement, and maintain a PPP or alternative documents that, when combined, meet the intent of the PPP.

1.4.　機密情報の保全関連

1.4.2.　施設クリアランス有の場合には、その区分、調査事項と方法、有効期限等

○ENCLOSURE 4 ではGSSO またはCPSO はSOP を準備しPSO に転送する。SOP は、DD Form 254 およびSCG による特別なセキュリティ規則。 DD フォーム254 及び契約に組み込まれているセキュリティポリシーに準拠して、特別なセキュリティ指導が実施される。

SOP においては、（1）一般規定と要件。　（2）報告要件。　（3）セキュリティクリアランス。　（4）SETA プログラム。　（5）分類とマーキング。　（6）機密情報の保護。　（7）訪問および会議。　（8）外注。　（9）情報セキュリティが織り込まれる。その他共同利用協定が規定され、ENCLOSURE 11 では契約そのものについて述べられ様式254 に関すること、請負業者独自研究、FOCI(外国影響)、契約完了時処理について規定している。

ENCLOSURE 4
GENERAL PROVISIONS AND REQUIREMENTS

1. SOP.

a. The GSSO or CPSO will prepare SOPs to implement the security policies and requirements unique to their facilities and the SAP.

b. The GSSO or CPSO will forward the proposed SOPs and SOP changes to the PSO, for approval.

c. A SOP is not required for a pre-solicitation activity, a research and development announcement, a request for information, or a request for proposal when there is no contractual relationship established for that effort or when contractors perform SAP work at government facilities only and not at contractor facilities. In these instances, classification guidance and special security rules reflected on the DD Form 254 and in the Security Classification Guide (SCG) suffice as the SOP.

d. Special security instructions will be instituted outlining the procedures that protect the information and are compliant with the security policy reflected on the DD Form 254 and expressly incorporated into the contract.

e. A SOP template is posted on the DSS website at http://www.dss.mil/isp/specialprograms.html. At a minimum, the following topics will be addressed in the SOP:

(1) General provision and requirements.
(2) Reporting requirements.
(3) Security clearances.
(4) SETA program.
(5) Classification and markings. 0
(6) Safeguarding classified information.
(7) Visits and meetings.
(8) Subcontracting.
(9) ISs.

4. CO-UTILIZATION AGREEMENT (CUA). The CUA documents areas of authorities and responsibilities between cognizant security offices (CSOs) when they share the same SAPF. A CUA will be executed between CSOs. The first CSO in an area, unless otherwise agreed upon, will be considered the host CSO responsible for all security oversight. The CUA will be initiated by the tenant PSO and approved by all parties before introduction of the additional SAP(s) into the SAPF.

a. Topics to be included in a CUA include: compliance inspection responsibility, incident notification, and host-tenant agreement to clarify inspection responsibilities. All CUAs will be reviewed and updated on a biannual basis.

b. Agencies desiring to co-utilize a SAPF will accept the current accreditation of the cognizant agency. Prospective tenant activities will be informed of all waivers to the requirements of this manual before co-utilization. Any security enhancements required by an agency or department requesting co-utilization should be funded by that organization and must be approved by the appropriate CA SAPCO before implementation. Any changes to the approved CUA must be submitted to the appropriate PSOs before implementing the changes.

c. For CUAs, the responsible organization will be identified for executing security cognizance with a carved-out SAP.

d. Co-utilization of Sensitive Compartmented Information (SCI) within a SAPF, or SAP within an SCI facility, will require authorization from the PSO and the servicing special security officer in accordance with Volume 2 of DoD Manual (DoDM) 5105.21 (Reference (l)).

ENCLOSURE 11 : CONTRACTING

1. CONTRACT SECURITY CLASSIFICATION SPECIFICATION (DD FORM 254) REQUIREMENTS. The government contracting officer (GCO) awards contracts on behalf of the government and coordinates security requirements with the PSO. The PSO or designee prepares the DD Form 254. The GCO or designee signs as the certifying official for each prime contract. For subcontracts, the prime CPSO or designee prepares a DD Form 254 and forwards it to the PSO for review before release to subcontractors. Lengthy attachments to DD Form 254 that merely repeat information, policy, and procedures contained in any other security directives should not be included.

a. SAP security guidelines, in addition to all collateral and SCI requirements, will be provided in the DD Form 254.

b. The activity will notify the CA SAPCO if a government official imposes any security requirements exceeding those provided for in this manual. The activity will make the notification through the GCO who will generate a memorandum for signature by the CPM addressing the issues to the CA SAPCO.

2. CLEARANCE STATUS OF SUBCONTRACTORS. If a subcontractor does not have the requisite FCL, the prime CPSO or designee will submit a FCL request to DSS in accordance with Reference (e). Subcontractor personnel will have the appropriate PCL in accordance with Reference (e).

3. SECURITY AGREEMENTS AND BRIEFINGS.

a. A prime contractor is responsible for issuing contracts and entering into a formal relationship with the prospective subcontractor. The prime contractor will obtain approval from the PSO before any release of SAP information. When conducting business with non-SAP briefed subcontractors, prime contractors will ensure SAP information is not inadvertently released. Any relationship with a prospective subcontractor requires prior approval by the PSO. The PSO will ensure that the association with the government activity or any SAP capability is not disclosed.

b. Prior to the release of any SAP information, the prime contractor must brief any prospective subcontractor regarding the procurement's enhanced special security requirements. Arrangements for subcontractor SAP access will be pre-coordinated with the PSO. The CPSO will complete a subcontractor or supplier data sheet for submission to the PSO. Discussions with prospective subcontractors may occur provided the discussions are limited to general interest topics without association to the government agency and scope of effort. The CPSO will include the reason for considering a subcontractor and attaches a proposed DD Form 254 to the subcontractor or supplier data sheet. The DD Form 254 will be tailored to be consistent with the proposed support being sought and be classified based on its content.

4. INDEPENDENT RESEARCH AND DEVELOPMENT (IR&D). The use of SAP information for a contractor IR&D effort occurs only with the specific written permission of the GCO. Procedures and requirements necessary for safeguarding SAP information is outlined in the DD Form 254 prepared by the PSO or designee. A letter defining the authority to conduct IR&D, a DD Form 254, and appropriate classification guidance will be provided to each contractor. Subcontracting of IR&D efforts will follow the same process as outlined in paragraph 1 of Enclosure 11 of this volume. IR&D operations and documentation that contain SAP

information are subject to inspection in the same manner as other SAP classified information in the possession of the contractor.

5. FOCI. All SAP(s) follow established FOCI procedures outlined in Volume 3 of DoDM 5220.22 (Reference (aa)).

6. NATIONAL INTEREST DETERMINATION (NID). In accordance with section 2004.22 of Title 32, Code of Federal Regulation, (Reference (ab)) a NID is required before authorizing any contractor cleared or presently in process for an FCL under a special security agreement (SSA) access to SAP information or any other proscribed information. A NID does not authorize disclosure of SAP information to a foreign government, a non-U.S. citizen, or a non-U.S. entity. Approval of NIDs are based upon an assessment of whether the release of SAP information is consistent with the national security interests of the United States. The requirement for a NID applies to new contracts, including pre-contract activities in which access to proscribed information is required, and to existing contracts when contracts are acquired by foreign interests and an SSA is the proposed foreign ownership, control, or influence mitigation method.

7. DISPOSITION AND CLOSE-OUT ACTIONS.

   a. CPSOs or designee will inventory, dispose of, request retention, or return for disposition all SAP material at contract completion or close-out. Request for proposals, solicitations, or bids and proposals contained in SAP files will be reviewed and screened by CPSOs in accordance with DoD Component records disposition instructions. Disposition of information by document control number will be submitted to the PSO and GCO for concurrence. Upon contract closeout, requests for retention of classified information will be submitted to the GCO through the PSO for review and approval. The contractor will not retain any SAP information unless specifically authorized in writing by the GCO. A final DD Form 254 will be issued for the storage and retention of SAP material. Storage and control requirements will be approved by the PSO.

   b. At the initiation of a closeout, termination or completion of a contract, the CPSO will consider actions for disposition of residual hardware, software, documentation, SAPF, and personnel accesses documented in a termination plan for approval by the PSO. The master classified material accountability record (log or register) will be transferred to the PSO at SAP closeout. All close out actions require final approval from the GCO and PSO.

1.4.3. 監査又は認証（有の場合には、その方法）

○4 タイプの監査①最低 2 年毎の主監査、それで問題だと②全体監査そこで見つかった部分の③再検査、これらと別の④抜き打ち監査。内部監査は毎年行い是正措置の不備な部分などを報告。必要に応じてアシスタントが訪問し支援と指導。評価は 5 段階評価で上位 3 段階だと 2 年サイクル、下から 2 番目だと 30 日以内レポート 90 日以内再検査スケジュール、最低評価だと 10 日以内レポート 90 日以内レビュースケジュール。

ENCLOSURE 9
SAP COMPLIANCE INSPECTIONS

1. GENERAL. The SAP security compliance process represents a unified and streamlined approach to the SAP security compliance inspections. All SAPs will be subject to the security compliance inspection process. The detailed guidance, procedures, and Security Inspection Checklist for conducting security compliance inspections are posted on the website http://www.dss.mil/isp/specialprograms.html.

2. INSPECTION TYPES. Inspections are conducted to validate that SAP security processes and procedures are in compliance with the governing DoD policies and to ensure that the risk of compromise to SAP information is at a minimum. Inspections should be executed with the least amount of impact to the SAP, while maintaining a proficient, equitable, and comprehensive review.

a. There are four possible types of external inspections that can be conducted.

(1) Core compliance inspections will be conducted at the direction of the inspection official, at a minimum every 2 years. The core compliance inspection consists of:

(a) Self-inspection checklist

(b) Core functional areas (CFAs)

1. TS SAP data and materials accountability

2. SETA

3. Personnel security
4. Security management and oversight
5. Cybersecurity
6. Physical security

(c) Special emphasis items (SEIs)

(2) Full scope inspections require a 100 percent validation of all functional areas. A full scope inspection will be conducted at the direction of the CA SAPCO when a less than satisfactory overall rating has been received as a result of a core compliance inspection. The most serious security rating, an unsatisfactory rating, is assigned when circumstances and conditions indicate that the program management personnel within the SAPF have lost, or are in danger of losing, their ability to adequately safeguard the classified material in their possession or to which they have access.

(3) Re-inspections are required when a less than satisfactory rating in one or more functional areas has been received. This can include just one or all functional area(s), SAP(s), or SEI(s). The re-inspection will be conducted no later than 90 days from the issuance of the final report.

(4) Unannounced or No Notice inspections can be full-scope or core compliance inspections conducted without notice and at the discretion of the CA SAPCO or designee.

b. A security representative from the prime contractor should be present and participate during inspections of subcontractors. Designated personnel will serve as inspection team chiefs, assign ratings, conduct in or out briefings, or be responsible for completing the security inspection report.

c. Inspections will be coordinated among the SAPCOs and DSS when not carved out and conducted jointly to the greatest extent possible. Compliance inspections involving multiple SAP organizations will be fully coordinated between participating DoD organizations by the assigned team chiefs. Each organization is responsible for publishing its report.

3. SELF-INSPECTION. Self-inspections are required to be conducted annually by the GSSO, CPSO or designee, for all SAPFs for which they are assigned responsibility. Utilize the security compliance inspection template and document any deficiencies in a corrective action plan that addresses the plan for correcting

deficiencies and areas deemed unsatisfactory as noted in the report. All supporting information will be included in the self-inspection report.

a. The documented results of self-inspections will be retained until the next government inspection is completed. All outstanding items must be completed before the destruction of any compliance documentation.

b. The documented results of the self-inspections will be submitted to the PSO for coordination within 30 days of completion. The PSO will be notified immediately if the selfinspection discloses the loss, compromise, or suspected compromise of SAP information.

c. In addition to the CFAs, inspectors will be required to validate SEIs. The CA SAPCO will annually determine the SEIs and report to the DoD SAPCO. The CA SAPCO will provide input on the trends and recommendations of the prior year to the DoD SAPCO.

4. STAFF ASSISTANCE VISIT (SAV). During a SAV, the PSO or designee will review security documentation and provide assistance and direction as necessary.

a. SAVs should be conducted as required and may include:

(1) Self-inspection checklists and corrective action plans.

(2) Outstanding government action items.

(3) Administrative security documentation (i.e., SOP, CPSO and IA manager appointment letter, OPSEC plan).

(4) Violations and infractions.

(5) SAP-specific CI trends and briefings.

(6) SETA program.

(7) Physical security standards.

(8) Cybersecurity.

(9) TS accountability.

b. The PSO will provide a SAV report to the GSSO or CPSO detailing what was covered and identifying all actions requiring resolution. During this visit, the PSO will provide guidance and direction to the organization, which will assist in the development of an effective and standardized security program. The PSO will annotate and address any concerns that require follow up before the next inspection.

5. DEFICIENCIES. Once the inspection has been completed, the team chief will determine the rating of the inspection based on the number of deficiencies identified and the risk of a compromise to classified information. Deficiencies will be defined as a finding or deviation.

6. RATINGS. Inspection ratings are superior, commendable, satisfactory, marginal, and unsatisfactory.

   a. If the rating is superior, commendable, or satisfactory, the inspection official will discuss any deficiencies that may have been identified and provide the final inspection results in the SAP review report within 30 days and place the organization on an inspection cycle not to exceed 24 months.

   b. If the rating is marginal, the inspection official will discuss any deficiencies that may have been identified and provide the final inspection results in the SAP review report within 30 days and schedule a re-inspection on the marginal areas within 90 days.

   c. If the rating is unsatisfactory, the inspection official will discuss any deficiencies that may have been identified and provide the final inspection results in the SAP review report within 10 days and schedule a compliance security review to be conducted within 90 days.

1.4.4. 機密情報の管理（人・施設）

○まずENCLOSURE 4の6ではOPSECに従っていること、10で脅威の提供や保護強化の支援を受けることが出来ること、11で特別な通話チャネルが使われることが述べられる。そしてENCLOSURE 5でその通話チャネルの詳細、保管管理、証跡、年次棚卸、秘密付随材、伝送・移動、公開、複製、破棄などが、更にENCLOSURE 10で立入について規定している。

ENCLOSURE 4
GENERAL PROVISIONS AND REQUIREMENTS

5. OPSEC. All SAPs will have an OPSEC program developed and maintained in accordance with DoDD 5205.02E (Reference (m)).

10. CI SUPPORT.

a. Analysis of foreign intelligence threats and risks to SAP information, material, personnel, and activities will be undertaken in accordance with DoDD O-5240.02 (Reference (o)); by the organic CI organization or by the lead military department CI organization in accordance with DoDI 5240.10 (Reference (p)). Information that may have a bearing on the security of a SAP will be provided by the government or military CI agency to the affected SAP PM and PSO, as necessary.

b. Contractors may use CI support to enhance or assist security planning and safeguarding in pursuit of satisfying contractual obligations. Requests for SAP-applicable CI support will be made to the respective PSO before contractors receiving such support.

11. COMMUNICATIONS SECURITY. SAP information will be electronically transmitted by approved secure communications channels authorized by the SOP.

ENCLOSURE 5
SAFEGUARDING CLASSIFIED INFORMATION

1. HANDLE VIA SPECIAL ACCESS CHANNELS ONLY (HVSACO).

a. The purposes of HVSACO are:

(1) To preclude the disclosure of general program-related information outside established acknowledged and unacknowledged SAP channels.

(2) To minimize OPSEC indicators.

(3) To facilitate communication of information within SAPs.

b. Dissemination of information warranting HVSACO protection will be limited to persons briefed into a SAP and retained within SAP approved channels. Formal SAP indoctrination or execution of briefing or debriefing forms specifically for HVSACO is not required. The term SAP channels denote secure, approved SAP communications systems, SAPFs, or PSO-approved SAP storage areas. HVSACO is not a classification level, but rather a protection or handling system.

Examples of HVSACO uses may include:

(1) For general non-program specific communications between and within SAPs. More specifically, on information related to SAP security procedures, test plans, transportation plans, manufacturing plans, and notional concepts related to research, development, testing, and evaluation of SAPs.

(2) When a paragraph or document contains information that is unique to a SAP and its distribution.

(3) When necessary to protect sensitive relationships.

(4) To protect information that does not warrant classification under Executive Order 13526 (Reference (t)).

(5) When using a SAP nickname for an unacknowledged SAP.

c. Upon request for public release, the originator of the material must review the material involved to determine whether to retain it within program channels:

(1) If public release is appropriate, remove the HVSACO marking from the document; or

(2) Inform the requestor of the decision not to release the information, citing an appropriate authority.

d. Training on HVSACO should be included in annual security awareness refresher sessions.

e. Procedures for the use of HVSACO should be included in Program SCGs.

f. Materials warranting HVSACO protection must be stored in accordance with the SOP. Unclassified HVSACO materials may be stored openly within an approved SAPF taking into account OPSEC considerations. PSOs may grant an exception to allow the taking of unclassified HVSACO materials to alternate temporary storage areas, provided the material is under an appropriately authorized individual's direct control, or under “key lock protection” which is controlled by that individual.

g. Transmission of SAP material.

(1) At a minimum, use U.S. First Class mail for shipment of unclassified materials requiring HVSACO protection.

(2) Use the secure mode when discussing HVSACO-protected material on

authorized telephones.

(3) Use only approved, secure facsimile (FAX) equipment when transmitting HVSACOprotected material.

(4) Do not transmit HVSACO-protected material via unclassified e-mail.

h. Reproduce unclassified HVSACO-protected information only on equipment approved by the PSO.

i. HVSACO protection does not require accountability. Document accountability is based on classification level or unique program requirements. Document control numbers, entry into document control systems, or internal or external receipts are not required for unclassified HVSACO-protected material.

j. Destroy HVSACO-protected information according to the procedures approved for classified material. Destruction certificates are not required for non-accountable HVSACOprotected materials.

k. Based on an assessment of the OPSEC risk, notify the PSO within 24 hours of any possible improper handling or misuse of HVSACO-protected information and its impact. An inquiry should be conducted to determine if a compromise occurred as a result of practices dangerous to security. The PSO will ensure that prompt corrective action is taken on any practices dangerous to security.

l. Contact the originating office for permission to remove HVSACO markings.

2. USE OF SECURE ENCRYPTION DEVICES AND ELECTRONIC TRANSMISSION EQUIPMENT.

a. Secure Encryption Devices.

(1) SAP government and industry organizations must use National Security Agency/Central Security Service (NSA/CSS) approved or certified Type I encrypted secure communications for the electronic transmission of all classified information.

(2) All products used for the electrical transmission of classified or sensitive information must be used in accordance with prescribed national and associated policies or doctrine.

b. Secure FAX. Secure FAX encrypted communications equipment may be used for the transmission of SAP information. When secure FAX is permitted, the PSO will approve the system in writing.

(1) Do not use FAX terminals equipped with the automatic polling function enabled unless authorized by the PSO.

(2) When approved by the PSO, SAP documents classified SECRET (S) SAP and below may be receipted via an automated generated message that confirms undisturbed transmission and receipt. A transmission log will be maintained and validated during GSSO or CPSO selfinspections and made available for review during inspections.

(3) When transmitting TS SAP documents over a secure FAX terminal, the recipient must acknowledge receipt of the TS SAP material. The recipient will return a signed receipt after completion of transmission. The transmission and receipt of TS material will be recorded by the sender in a FAX log.

c. Electronic Transmission. When using electronic transmission (e.g., voice over internet protocol, video teleconferencing for SAP material), encrypted communications equipment will be used. When secure electronic transmission is permitted, the authorizing official, in coordination with the PSO, will approve the system in writing to the GSSO or CPSO.

3. CONTROL. SAP classified material, hardware, equipment and all media not subject to accountability will be controlled by the procedures implemented by policy, training, and awareness that:

a. Regulate and monitor the introduction and exit of all controlled items from all SAPFs.

b. Identify and document:

(1) The identity of the custodian, date created (or entered the SAPFs) and date destroyed (or exited the SAPFs).

(2) Classification, Program sensitivity (e.g. TS, S//SAR-XYZ, U//HVSACO, For Official Use Only (FOUO), Unclassified (U), personally identifiable information).

(3) Type (e.g. documents, hard disks, compact disks, universal serial bus storage devices).

(4) Content (e.g., application software, non-writable or writable, engineering notebook).

c. At least on an annual basis, the continued need for all controlled items will be assessed and items no longer required will be destroyed.

d. Safeguarding of classified information, to include SAP material, will be done in accordance with Volume 3 of DoDM 5200.01 (Reference (u)), unless otherwise noted in this volume.

4. ACCOUNTABILITY.

a. An accountability system approved by the PSO will be developed and maintained for the following SAP classified information.

(1) All TS SAP material, media, hardware, equipment, etc.

(2) S SAP material, media, hardware, equipment, etc. when directed by the CA SAPCO.

(3) All other classified media when directed by the CA SAPCO.

b. Accountable SAP material will be entered into an accountability system whenever it is received, generated, reproduced, or dispatched either internally or externally to other SAPFs. The accountability system will be designed to record all transactions of handling, receipt, generation, reproduction, dispatch, or destruction. The accountability system will assign individual responsibility for all accountable information. An automated system, if used, will have a backup. When SAP material is received with the originator's accountability control number, the accountability system will include the originator's accountability control number.

c. The accountability system will have at the minimum:

(1) Classification.

(2) Originator of the item.

(3) Title and description of item.

(4) Custodian assigned.

(5) Date of product.

(6) Control number (maintained in consecutive number series).

(7) Copy number.

(8) Page count.

(9) Disposition and date.

(10) Destruction date.

(11) Internal and external receipt records

d. A disclosure sheet will be maintained for each TS item. The name is recorded only once regardless of the number of times subsequent access occurs. Once destruction of a TS product takes place, the TS access record will be kept with the destruction paperwork and destroyed 3 years after the document is destroyed.

e. Electronic files do not need to be placed into accountability systems or the information management system referenced in paragraph 4a of this enclosure when residing on ISs or receipted when transmitted between system users within the same unified network provided the data remains resident within the IS.

5. ANNUAL INVENTORY.

a. A 100 percent inventory of accountable SAP material will be conducted annually by the individual responsible for the control system or their alternate and a disinterested party. The annual inventory date will not exceed the previous year's inventory date by more than 12 months. Inventories will be conducted by visual inspection of all items of accountable SAP material and verification of pertinent information (originator, date, subject, file number, etc.) and page count for TS SAP held within the SAPF.

b. Inventories of TS material will be documented by the TSCO and a second disinterested individual and made available during security compliance inspections. Discrepancies will be reported immediately to the PSO, who will ensure action is taken, as appropriate, in accordance with Enclosure 8 of this volume.

6. COLLATERAL CLASSIFIED MATERIAL.

a. The PSO will provide oversight for collateral classified material maintained in the SAP. The process for introduction of collateral material will be approved by the PSO. Collateral material assigned or produced under a collateral contract required to support a SAP will be PSOapproved before the introduction, inclusion, or production, and may be transferred within SAP controls.

b. Transfer will be accomplished in a manner that will not compromise the SAP or any classified information. Collateral classified material generated during the performance of a SAP contract may be transferred from the SAP to another SAP or collateral program.

7. TRANSMISSION AND PREPARATION OF SAP CLASSIFIED MATERIAL.

a. SAP information will only be transmitted outside the SAPF using one of the methods identified within this section. The GSSO or CPSO will oversee transmission of SAP material. The order of precedence for transmission processes is:

(1) Cryptographic communications systems (i.e., secure facsimile, IS).
(2) Courier.
(3) PSO approved government or commercial carrier for S SAP material and below.
(4) Defense Courier Service for TS SAP material.
(5) United States Postal Service (USPS) registered mail or US Express Mail for S SAP material and below within the continental United States (CONUS).
(6) USPS certified mail for CONFIDENTIAL SAP material and below within CONUS.

b. SAP material being mailed or couriered will be prepared, reproduced, and packaged by the appropriately cleared SAP-briefed personnel inside the SAPF.
(1) Dispatch receipts are required for the transmission of SAP material.
(2) Classify receipts according to content.
(3) Inner and outer wrapping markings.

(a) Inner wrappings will be opaque and marked with the "TO" and "FROM" blocks and will bear the highest level of classification marking of the content.
(b) Outer wrappings will be opaque and will show an unclassified address on the "TO" and "FROM" blocks.

(4) When a receipt is not returned within 15 days, contact the recipient to determine status of the material. If the material is received, have the recipient provide the receipt. If the recipient did not receive the material, immediately initiate a preliminary inquiry and inform the PSO and the GPM.

c. SAP material will be transported from one SAPF to another in an unobtrusive and secure manner.

(1) Courier(s) must be accessed to the level of SAP being couriered.

(2) For local travel, SAP material may be hand-carried using a locked container as the outer wrapper. Local travel will be defined by CA SAPCO. Travel outside of the defined local area of the originating SAPF requires PSO approval. Attach a tag or label with the individual's name, organization, and telephone number.

(3) Travel should be performed using a personal, company owned, rented, or government vehicle. Use of public transportation requires PSO approval.

(4) TS SAP working papers taken to another SAPF in the same building for collaboration that will be returned before the expiration of the working paper time limits does not need to be placed into accountability when leaving the SAPF. Hand receipts documenting item and page count are still required.

d. When approved by the PSO, a USPS mailing channel may be established to ensure mail is received only by appropriately cleared and accessed personnel. Use USPS-registered mail or USPS Express Mail for S SAP material. Use USPS certified mail for CONFIDENTIAL SAP. "For Official Use Only" and unclassified HVSACO, material may be sent by First Class mail. When associations present an OPSEC concern in receiving and sending mail, the GSSO or CPSO will establish and use a sterile Post Office box with the written approval from the PSO.

(1) Except for TS SAP material, a USG-approved contract carrier (i.e., USPS Express Mail) can be used for overnight transmission on a case-by-case basis with approval of the PSO. Packages may only be shipped on Monday through Thursday and delivery date must be checked to ensure that the

carrier does not retain the classified package over a holiday or weekend.

(2) These methods of transmitting selected SAP information are in addition to, not a replacement for, other transmission means previously approved for such material. Use of secure electronic means is the preferred method of transmission.

(3) Except for approved USPS means, use overnight delivery only when:

(a) Written approval is received by the PSO.

(b) SAP requirements dictate.

(c) Essential to mission accomplishment.

(d) Time is of the essence, negating other approved methods of transmission.

(e) Receiver of material will be readily available to sign upon arrival.

(4) To ensure direct delivery to address provided by the PSO:

(a) Do not execute the waiver of signature and indemnity on USPS label.

(b) Do not execute the release portion on commercial carrier forms.

(c) Ensure an appropriate recipient is designated and available to receive material.

(d) Do not disclose to the express service carrier that the package contains classified material.

(5) Immediately report any problem, misplaced, or non-delivery, loss, or other security incident encountered with this transmission means to the PSO.

e. The GSSO or CPSO will provide detailed courier instructions and training to SAP-briefed couriers when hand-carrying SAP information. Problems encountered will be immediately reported to the PSO, who may authorize exceptions when operational considerations or emergency situations dictate. The following rules will be adhered to when couriering classified material:

(1) The responsible PSO is required to approve all couriering of TS SAP material. Twoperson courier teams are required for all TS SAP material unless a single courier is authorized in writing by the PSO. The courier must be accessed to the level of SAP information being couriered.

(2) A single-person courier may be used for S SAP and below materials.

(3) Provisions will be made for additional couriers and overnight storage, when required (regardless of classification), when it appears continuous vigilance over the material cannot be sustained by a single individual.

(4) As a minimum, the GSSO or CPSO from the departure location will provide each authorized courier with a copy of Department of Defense (DD) Form 2501, "Courier Authorization," based on instructions located at http://www.dtic.mil/whs/directives/infomgt/forms/forminfo/forminfopage1828.html or a PSO approved locally produced courier authorization memorandum.

(a) At a minimum, the courier authorization and instructions will address:

1. Method of transportation.
2. Travel itinerary (intermittent or unscheduled stops, remain-overnight scenario), specific courier responsibilities (primary or alternate roles, as necessary).
3. Completion of receipts, as necessary, and full identification of the classified data being transferred.
4. A discussion of emergency or contingency plans (include after-hours points of contact, primary or alternate contact data, telephone numbers).
5. Each courier will acknowledge receipt and understanding of this briefing in writing.

(b) Experienced SAP-briefed individuals who frequently or routinely perform duties as classified couriers may be issued courier authorization cards or DD Form 2501 by the GSSO or CPSO in lieu of individual letters for each trip. The form is issued for no more than 1 year at a time. The requirement for authorization to hand carry will be revalidated on at least an annual basis and a new form issued, if appropriate.

8. AIRPORT-SCREENING GUIDELINES FOR HANDLING CLASSIFIED MATERIAL.

a. Travel to and from locations in the U.S. aboard commercial or government carriers.

(1) PSOs will apprise couriers of the limitations and restrictions surrounding screening procedures. Notifying government screening officials of courier

status is not required until screening officials request to inspect classified material.

(2) When screening officials request to inspect classified material, couriers will:

(a) Allow the classified material to undergo the x-ray examination.

(b) Divest any material that may trigger the automated screening equipment.

(c) Place all metal objects and electronics on the x-ray belt or in a second bag.

(d) If the screening official desires to inspect the package after x-ray screening, the courier will:

1. Present the courier authorization letter and their government-issued identification.
2. Request assistance from the screening official's supervisor.
3. Request a private screening.
4. Permit the supervisor to inspect the outer package but not the contents. If the screening supervisor cannot determine if the material is cleared for transport, the courier will contact the originating PSO for further instructions.

b. Travel to or from locations outside the United States. Classified information will be sent via secure classified networks, classified FAX, or diplomatic pouch whenever possible. Handcarrying SAP material other than by diplomatic courier should be used only as a last resort. Couriering classified SAP material on commercial aircraft is only approved by waiver issued by the Director, CA SAPCO, or designee.

c. Transportation Security Administration (TSA) Guidelines. The TSA publishes airport screening guidelines for handling classified material. GSSOs and CPSOs will ensure couriers are aware of the limitations and restrictions surrounding screening procedures.

9. TRANSPORTATION PLANS. The GSSO or CPSO will develop a transportation plan coordinated with and approved by the PSO at least 30 days in advance of the proposed movement. The transportation plan must:

a. Appoint a SAP-accessed individual knowledgeable about SAP security requirements to serve as the focal point for transportation issues.

b. Ensure that the planning includes priority of transportation modes (government surface, air, commercial surface, air) and inventory of classified SAP material to ensure SAP integrity.

c. Maintain a continuous chain of custody between the origination and destination, and comply with all Department of Transportation laws and SAP security requirements.

d. Include contingency planning (a description of emergency procedures, and who is responsible for actions that must be taken in the event of an emergency, e.g., unexpected stop anywhere along the route). Identify individuals by name, and provide their organization, telephone and fax numbers, and e-mail addresses.

e. Ensure CI support is incorporated into transportation planning and execution.

10. RELEASE OF INFORMATION.

a. Public release of SAP information is not authorized without written authority from the government in accordance with subtitle A, part 1, chapter 2, section 119 of Title 10 United States Code (U.S.C.) (Reference (v)) and part 2, appendix d of Title 42 U.S.C. (Reference (w)). Personnel are responsible to report any attempt by unauthorized personnel to obtain SAP information immediately to the PSO to the GPM.

(1) Information concerning SAPs must not be released to any non-SAP-accessed individual, firm, agency, or government activity without SAPCO approval. Classified or sensitive information concerning SAPs must not be included in general or unclassified publications, technical review documents, or marketing literature.

(2) All material proposed for release will be submitted through the PSO to the GPM 60 days before the proposed release date. After approval is granted, additional case-by-case requests to release identical data are not required.

b. Personnel currently or previously accessed to a SAP will provide the GPM and PSO with a copy of any proposed intended release of information that could potentially contain SAP information for review before public release. Information considered for release such as models, software, and technology that may impact other SAPs will require additional coordination with the DoD SAPCO, and other Component SAPCOs before release. The information and materials proposed for release will remain within SAP security channels until authorized for release.

c. The Defense Technical Information Center or the U.S. Department of Energy Office of Scientific and Technical Information does not accept SAP information.

d. Each SAP security officer will ensure the area SOP contains a process to ensure documents such as award nominations, performance reports, evaluations, etc. are reviewed to eliminate any program sensitive information before further dissemination.

11. REPRODUCTION.

a. SAP information will only be reproduced on equipment approved by the PSO. The GSSOs or CPSOs will prepare written reproduction procedures, and post a notice indicating if equipment can or cannot be used for reproduction of classified SAP material within a SAPF, and who is authorized to reproduce such material. Maintenance procedures will be written and incorporated into the SOPs listing the actions necessary when non-SAP briefed maintenance technicians' work on the equipment. When possible, an additional hard drive for maintenance purposes only should be purchased.

b. Equipment may be used outside a SAPF (e.g., within a SAP working area), provided written procedures are approved by the PSO which will include procedures for clearing of equipment, accessing of operators, clearing of media, handling malfunctions. GSSOs or CPSOs will position reproduction equipment to be continually monitored when it is outside a SAPF to achieve a risk mitigated solution. All reproduction equipment will be in compliance with applicable ISs guidance.

12. DESTRUCTION. Accountable SAP material will be destroyed using two SAP-briefed employees with access to the level of material being destroyed. Non-accountable SAP material may be destroyed by a single SAP-briefed

employee with access to the level of material being destroyed. All classified waste containing SAP information will be destroyed as soon as possible. Such materials must not accumulate beyond 30 days unless approved by the PSO. NSA/CSS-approved equipment and their destruction procedures will be used to destroy SAP material as authorized by the PSO. Destruction of non-standard SAP materials will be approved by the PSO. Accountable and non-accountable SAP material will be maintained in accordance with the DoD Components record management manuals and instructions.

a. Prepare certificates of destruction itemizing each accountable document or material destroyed, to include citing the appropriate document control and copy number. For accountable SAP material, destruction certificates must be completed and signed by both of the individuals involved in the destruction immediately after destruction is completed.

b. Public destruction facilities may be used only with the approval of and under conditions prescribed by the PSO.

ENCLOSURE 10
VISIT REQUEST PROCEDURES

1. GENERAL. Approval by the appropriate GPM or designated representative is required for all visits to SAP activities except for visits between the sites of a prime contractor and the prime's subcontractors, which may be approved by the CPM, or designee. A written or electronic visit notification must be approved before visiting a SAPF. Centralized personnel security databases may be used for access verification if authorized in writing by the responsible PSO or CA SAPCO, however GPM or designated representative approval of the visit is still required. All visit requests will be transmitted via PSO-approved channels.

2. ADVANCED NOTICE. SAP accessed personnel must make every effort to provide advance notification of the visit to their GSSO or CPSO. Visitors who courier classified material will provide travel itinerary, storage requirements, and emergency contact information to their GSSO or CPSO and the destination GSSO or CPSO.

3. UNANNOUNCED AND NON-VALIDATED ARRIVALS. Access will be denied if a

visitor arrives at a government or contractor SAPF without verification of the requisite SAP accesses, except for the PSOs and supporting security staff members (as designated by the PSO) who may visit all SAPFs under their responsibility without furnishing advanced notification.

4. DURATION. Visit request authorizations in excess of 12 months are not permitted unless approved in writing by the PSO.

5. VALIDATION OF VISITOR'S IDENTIFICATION. The positive identification of each visitor will be made using an authorized credential in accordance with Directive-type Memorandum (DTM) 09-012 (Reference (z)); the identification number of the credential to be used will be annotated on the visit request. Federal Government-affiliated identification cards will not be used for positive identification in unacknowledged locations.

6. ESCORTING OF VISITORS.

   a. Only resident SAP-accessed personnel can escort and closely control movement of nonSAP accessed visitors requiring access to a SAPF. The number of escorts required will be dependent upon the number of visitors and the capability of closely monitoring the visitor activities.
   b. Foreign nationals visiting a SAPF will be approved by the CA SAPCO or designee.
   c. The PSO or designee will determine whether an internal warning system (such as rotating light beacons) is necessary to warn accessed occupants of the presence of non-briefed personnel. The PSO or designee will employ other or additional methods (e.g., verbal announcements), as required, to warn or remind personnel of the presence of non-briefed personnel.

7. TERMINATION OR CANCELLATION OF A VISIT REQUEST. If a person is debriefed from the SAP before expiration of a visit request authorization, or if cancellation of a current visit request authorization is otherwise appropriate, the security officer or their designated representative will immediately notify all recipients of the cancellation or termination of the visit request authorization.

8. VISITOR RECORDS. Unless a PSO approved electronic visitor record is on file,

the security officer will maintain segregated visitor logs for non-briefed and SAP accessed personnel. The visitor record will contain the visitor's:

a. First and last name.
b. Organization or firm.
c. Date visited.
d. Time in and out.
e. Sponsor.
f. Identification number of authorized credential in accordance with Reference (z).
g. Citizenship.
h. Purpose.

9. CONGRESSIONAL VISITS. The CA SAPCO will provide guidance when a congressional visit to a SAPF is proposed. In the event of the unannounced arrival of a congressional delegation, DoD employees accessed to DoD SAPs will contact the PSO for guidance. The PSO will contact the CA SAPCO for instructions. All communications and information flow between the authorized congressional members or their staff will be coordinated through the DoD SAPCO and CA SAPCO.

10. UNFORESEEN OPERATIONAL OR EMERGENCY SITUATIONS. When unforeseen events prevent providing a written or electronic visit notification, visit approval may be provided telephonically by the PSO or designee. Written certification and confirmation will follow verbal authorization within 24 hours.

1.4.5. 情報セキュリティ

○ENCLOSURE 6 でサイバーセキュリティが述べられ、実装ガイド(JSIG)・DoD 8570.01-M, "Information Assurance Workforce Improvement Program,"・ CNSSP No. 22, "National Policy on Information Assurance Risk Management for National Security Systems,"・ DoD Directive 5205.07, "Spec DoD Instruction 5205.11, "Management, Administration, and Oversight of DoD Special Access Programs (SAPs)", ial Access Program (SAP) Policy,"・ Intelligence Community Directive Number 503, "Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation,"に従う。

ENCLOSURE 6
CYBERSECURITY

Reference (k) provides standardized cybersecurity related implementation guidance for policy and procedures for management of all networks, systems, and components at all classification levels for all DoD SAPs.

a. All DoD SAP ISs that receive, process, store, display, or transmit SAP information must operate in compliance this manual and References (h) and (k).
b. DoD SAP implementation of the Risk Management Framework, through the use of this manual, Annex B of Committee on National Security Systems Policy No. 22 (Reference (x)) and Reference (k) and in accordance with References (b) and (c), is aligned with Intelligence Community Directive Number 503 (Reference (y)).
c. Additional or compensatory technical and non-technical countermeasures may, after consultation with the Director of the CA SAPCO or designee, be imposed in the interest of SAP protection in coordination with the PSO.

1.5. 不正に対する対応（罰則や報告等）

○ENCLOSURE 4の2で報告要件、3で不正に対する内部告発手順、9で訴訟について規定しているが、セキュリティインシデントについてはENCLOSURE 8一章を割いている。

ENCLOSURE 4
GENERAL PROVISIONS AND REQUIREMENTS

2. REPORTING REQUIREMENTS. Reports required based on this volume are posted on the DSS website at http://www.dss.mil/isp/specialprograms.html. At a minimum, report the following to the PSO:

a. Adverse Information
b. Refusal to sign a SAP Indoctrination Agreement
c. Change in Employee Status
d. Employees Desiring Not to Perform on SAP Classified Work
e. Foreign Travel
f. Changes or modifications to the SAP area accreditation

3. FRAUD, WASTE, ABUSE, AND CORRUPTION (FWAC).

a. Government and industry FWAC SAP reporting involving SAP information will be accomplished through SAP channels. Collateral FWAC reporting channels must not be used for SAP information.

b. The PSO will provide the telephone number for the current FWAC hotline for reporting SAP information. FWAC reporting information will be conspicuously posted in the SAP workspace.

c. Employees do not need management approval before making reports.

9. LITIGATION AND PUBLIC PROCEEDINGS.

a. Threatened or actual litigation, administrative investigations or inquiries, or public proceedings at the international, federal, State, tribal, or local levels that may involve a SAP will be reported to CA SAPCO. Appropriate DoD general counsel offices or judge advocate offices will be notified of potential litigation issues at the earliest possible time. These proceedings include legal or administrative actions in which the prime contractor, subcontractors, or government organizations and SAP-accessed individuals are a named party (plaintiff, defendant, or witness).

b. DoD government and contractor personnel accessed to DoD SAPs will inform the PSO of any litigation actions that may pertain to the SAP, to include litigation regarding the physical environments, facilities, or personnel, or as otherwise directed by the GPM. PSOs will be notified of employee or union strikes, employer discrimination complaints, Equal Employment Opportunity cases, Merit Service Protection Board appeals, litigation, etc. in accordance with the timelines required by Enclosure 2, paragraph 5.s of Reference (c).

ENCLOSURE 8
SECURITY INCIDENTS AND INQUIRIES

To ensure the protection of classified information to include classified information protected by SAPs, security incidents will be investigated and actions will be taken to ensure that the adverse effects of loss or compromise of classified information are mitigated. Security incidents involving classified information will be handled and investigated in accordance with this manual and References (b) and (u).

a. All security violations will be reported immediately, to the extent possible, and no later than 24 hours of discovery, to the PSO, through the procedures described in this enclosure.

b. The PSO, through the chain of command, will advise the CA SAPCO in all instances where national security concerns would impact any security program or personnel security clearances (PCL) of SAP-accessed individuals. The PSO will notify and report security violations to the GPM with a copy of the report to the appropriate CA SAPCO. The security official of the affected SAPF will recommend the scope of the corrective action taken in response to the violation and report it to the PSO for approval.

c. Actual or potential compromises involving DoD SAPs, the results of the compromise or inquiries, and investigations that indicate weaknesses or vulnerabilities in establishing SAP policy, or procedures that contributed to an actual or potential compromise will be reported to the CA SAPCO, Original Classification Authority, and the DoD SAPCO, who will report to the Director of Security Policy and Oversight, Office of the USD(I).

d. Personnel determined to have had unauthorized or inadvertent access to classified SAP information:

(1) Will be interviewed by the GSSO, CPSO, or PSO to determine the extent of the exposure.

(2) May be requested to complete an inadvertent disclosure statement. An inquiry will be conducted to determine the circumstances of the inadvertent disclosure.

e. Guard personnel or local emergency authorities (e.g., police, medical, fire) inadvertently exposed to SAP material during an emergency response situation will be interviewed by the GSSO, CPSO, or PSO to determine the extent of the exposure.

(1) The PSO will determine if an inquiry is required by Reference (u) to determine whether or not there was a loss of classified information or whether or not unauthorized personnel had, or could have had, access to the information.

(2) The inquiry identifies the facts, characterizes the incident as an infraction or a violation, and identifies, if possible, the cause(s) and person(s) responsible, reports corrective action or a requirement for an investigation.

f. Refusal to sign an inadvertent disclosure statement by personnel inadvertently exposed to classified information will be reported by the GSSO or CPSO to the PSO by the next duty day.

1.6. 他組織（又は国）との相互認証

○ENCLOSURE 4 では 7 で知的財産権、8 で武器管理、12 で国際関連について規定し、ENCLOSURE 12 では技術移転に一章使っている。

ENCLOSURE 4
GENERAL PROVISIONS AND REQUIREMENTS

7. PATENTS AND INTELLECTUAL PROPERTY. The CA SAPCO will develop procedures for processing patents and intellectual property involving SAP(s).

8. ARMS CONTROL AND TREATIES.

a. DoDD 2060.1 (Reference (n)) establishes the arms control implementation and compliance responsibilities for SAPs; in accordance with Reference (b), treaty compliance requirements, obligations, or constraints will be considered as an integral part of the policy. DoD SAPs must be prepared to comply with treaties and agreements to which the USG is a signatory. DoD SAPs will be protected against unnecessary or inadvertent exposure during USG participation in authorized verification activities, confidence-building measures, and over flights.

b. The PSO, GSSO, and CPSO should be familiar with various arms control verification activities in order to exercise security oversight for SAPs. Arms control treaty guidance and procedures are located at the website http://www.dss.mil/isp/specialprograms.html.

12. INTERNATIONAL SAP SECURITY REQUIREMENTS.

a. The National Disclosure Policy (NDP-1) (Reference (q)) governs all foreign disclosures of classified military information. Security planning for foreign disclosure is an ongoing process that requires reviews at each milestone in the SAP lifecycle.

(1) All SAPs will comply with Reference (q). SAPs will include foreign disclosure and security planning at the beginning of the prospective SAP process or at the earliest possible date foreign disclosure is identified in an ongoing SAP. When a SAP is identified for international cooperation or foreign disclosure, all foreign disclosure and policy guidance will be in accordance with Reference (q), DoDD 5230.11 (Reference (r)), and DoDD 5530.3 (Reference (s)).

(2) The foreign disclosure officer and CA SAPCO do not have authority to disclose SAPs without Secretary of Defense or Deputy Secretary of Defense approval, in accordance with Reference (b).

b. The GPM and PSO will coordinate with their Component Foreign Disclosure Office and CA SAPCO to develop technology assessment or control plans, MOAs, and security documentation for all international SAPs as appropriate. Additional security requirements are further identified in bilateral program-specific security agreements, General Security of Military Information Agreements, and Industrial Security Arrangements.

ENCLOSURE 12
SAP TECHNOLOGY TRANSFERS

1. TECHNOLOGY TRANSFERS. Two primary issues must be addressed with all technology transfers. The first is to ensure that the scope of the gaining SAP SCG is sufficient to protect technology that is to be transferred. If not, the gaining SAP SCG must be updated (approved before transfer), or the transfer should not occur. The second issue is to ensure all technology to be transferred is reviewed to determine if there are any proprietary or data rights associated with the technology proposed for transfer. If so, those specific items must be clearly annotated with

the appropriate data rights. The technology transfer agreement (TTA) is used to document transfers of SAP technology between U.S. government agencies. GPMs from both SAPs should maintain records of all technology transfers. TTAs can only be approved by the CA SAPCO or authorized designee. Transfers of SAP technology to a foreign government will be conducted in accordance with Foreign Disclosure Procedures in Reference (c).

2. SYSTEM OR CAPABILITY TRANSFERS. A system or capability transfer MOA will be prepared by the GPM, GSSO, and PSO for any system or capability transferred to or from a DoD Component from or to another DoD Component or non-DoD organization when the system or capability to be transferred requires continued resources to sustain. The system or capability transfer MOA must be approved by the CA SAPCO. The system or capability transfer MOA must include:

a. Description of technology to be transferred (i.e., data, knowledge, equipment).
b. Gaining and losing organizations.
c. Roles and responsibilities.
d. Gaining CSO.
e. Personnel security access requirements (if beyond standard requirements).
f. Logistics and sustainment requirements.
g. Marking guidelines and instructions.
h. Contracting review.
i. Legal review.
j. Resources necessary to sustain the SAP.

1.7. 人材育成の仕組み（情報保全のモニタリング要員等）

○ENCLOSURE 7 が security education and training awareness（SETA）についての章で、GSSO と CPSO によって確立され、PSO によって承認された SETA は SAP にアクセスする全ての個人に適用され毎年の研修がなされる。

ENCLOSURE 7
SETA PROGRAM

1. GENERAL. GSSOs or CPSOs will ensure that the SETA program meets the specific and unique requirements of this manual. The SETA program applies to all

SAP-accessed individuals. General, non-SAP specific, or company-wide security briefings may be used to form the basis for or supplement the SAP SETA requirement. Training on the unique, SAP, and SAPF specific parameters of the SAP is required.

2. PSOs. PSOs will approve the SETA program of assigned SAPs. This may be a standalone document or incorporated into the SAPF's SOP.

3. GSSO(s) AND CPSO(s). GSSO(s) and CPSO(s) will:

   a. Establish a SETA program for their SAP(s).
   b. Annotate compliance with SETA requirements in the annual self-assessment checklist and provide to the responsible PSO in accordance with this volume.

4. ANNUAL TRAINING.

   a. Activities that grant SAP access will ensure that accessed individuals receive annual training to reaffirm their responsibilities while accessed to a SAP. When major changes occur such as changes in the classification for information protected under a SAP, new SAP-specific information that requires protection will be updated in briefings and training.
   b. Annual training by the PSO, GSSO, CPSO, or designee may take several different forms, to include but not limited to face-to-face briefings, computer-based presentations sent via e-mail on the appropriate classified network, single page data sheets requiring individual review and signature, or other methods as approved by the PSO.

      (1) Annual training will be recorded by utilizing the SAP training record template posted on the DSS website at http://www.dss.mil/isp/specialprograms.html.
      (2) If multiple SAPs are involved, a centralized record system may be utilized as approved by the PSO.

   c. SAP-accessed individuals will be briefed by PSOs, GSSOs, and CPSOs on individual reporting requirements during initial briefings and during annual training in accordance with this manual.

1.8.　その他特徴的な部分

本ハンドブックは、自社営業秘密をどのように守るかをガイドする教育本的位置づけとなっている。

③　DoD Directive NUMBER 5143.01

Under Secretary of Defense for Intelligence (USD(I))

DOD の中では、Secretary of Defense for Intelligence（諜報担当国防次官）管掌の国防セキュリティサービス（DSS）が、国家産業セキュリティ･プログラムを管理し、国防の部分を実施する。

国防セキュリティサービス（DSS）は、4 つの実務ユニットを持っている。

□ 産業セキュリティフィールド･オペレーションズ (ISFO) □ 産業政策とプログラム (IP)
□ 防諜（CI） □ セキュリティ教育、研修および意識向上（SETA）

本指令はその Secretary of Defense for Intelligence の管掌と役割を指示する。

This directive:

a. Reissues DoD Directive (DoDD) 5143.01 (Reference (a)) to update the responsibilities and functions, relationships, and authorities of the USD(I), pursuant to the authority vested in the Secretary of Defense (SecDef) by sections 113 and 137 of Title 10, United States Code (U.S.C.) (Reference (b)), and in accordance with section 3001 et seq. of Title 50, U.S.C. (Reference (c)), as well as Public Law 108-458 (Reference (d)), Executive Order (E.O.) 12333 (Reference (e)), and E.O. 13470 (Reference (f)).

b. Authorizes the USD(I) to reissue chartering DoDDs, in accordance with DoD Instruction (DoDI) 5025.01 (Reference (g)), for OSD Presidentially-appointed, Senate-confirmed officials who are under the authority, direction, and control of the USD(I).

c. Conforms to and is consistent with law and Presidential guidance concerning the authorities and responsibilities of the Director of National Intelligence (DNI).

d. Cancels Deputy Secretary of Defense (DepSecDef) Memorandums (References (h) and (i)).

1.1.　組織体制（人事体制等）

○3. RESPONSIBILITIES AND FUNCTIONS.の中のまず冒頭で DIA、NGA 等とともに DSS がその管掌になること、b で SAP を保証すること、j の(6)で NISP に関する国防総省としてのすべての責任と義務を果たすことを諜報担当国防次官に与えている。

3. RESPONSIBILITIES AND FUNCTIONS. The USD(I) is the Principal Staff Assistant (PSA) and advisor to the SecDef and DepSecDef regarding Intelligence, Counterintelligence (CI), Security, sensitive activities, and other intelligence-related matters (referred to in this directive as "assigned responsibilities" or "Defense Intelligence, CI, and Security"). In this capacity, the USD(I) exercises SecDef authority, direction, and control over, and oversees the activities of, the Defense Intelligence Agency (DIA), the National Geospatial-Intelligence Agency (NGA), the National Security Agency/Central Security Service (NSA/CSS), the National Reconnaissance Office (NRO), and the Defense Security Service (DSS); and exercises planning, policy, and strategic oversight for all associated policy, plans, and programs. In the exercise of assigned responsibilities, the USD(I):

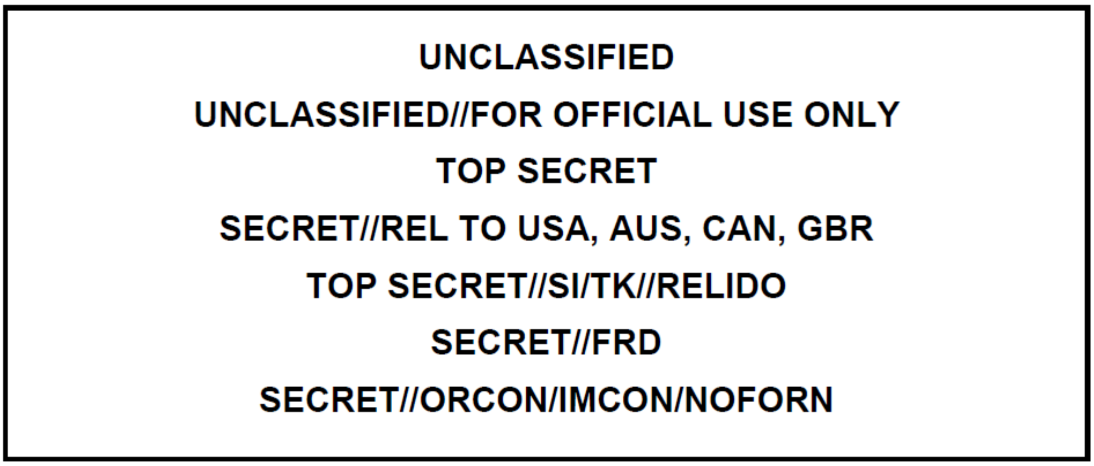
b. Engages the National Security Council (NSC) staff, other government agencies (OGAs), and DoD Components to develop policies, plans, and programs to enable operational application of Defense Intelligence and other capabilities, as appropriate. Provides the NSC principals and deputies committees with Defense Intelligence, CI, Security, sensitive activities, and special program perspectives in coordination with the Under Secretary of Defense for Policy (USD(P)). Ensures DoD intelligence and intelligence-related sensitive activities and special access programs (SAPs) align with SecDef and U.S. Government (USG) guidance.

j. For Defense Security Programs and associated matters:

(6) Performs all SecDef duties and responsibilities regarding the National Industrial Security Program, pursuant to E.O. 12829 (Reference (ad)). Develops industrial security policy and guidance, and oversees DoD implementation of Reference (y) and the DoD Industrial Security Program.

④　DoD Manual 5200.01: DoD Information Security Program

Figure 1. Examples of Banner Markings



UNCLASSIFIED

UNCLASSIFIED//FOR OFFICIAL USE ONLY

TOP SECRET

SECRET//REL TO USA, AUS, CAN, GBR

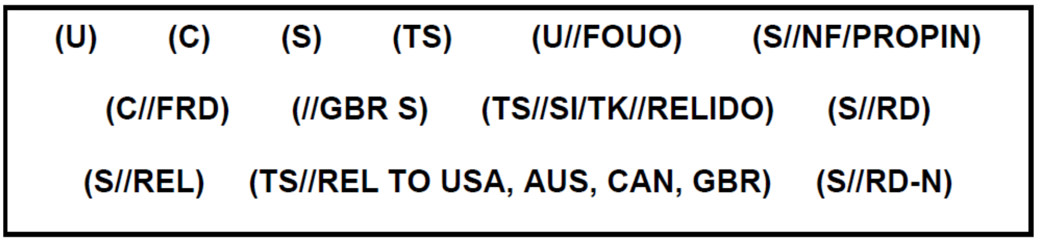
TOP SECRET//SI/TK//RELIDO

SECRET//FRD

SECRET//ORCON/IMCON/NOFORN

Figure 2. Examples of Portion Markings

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



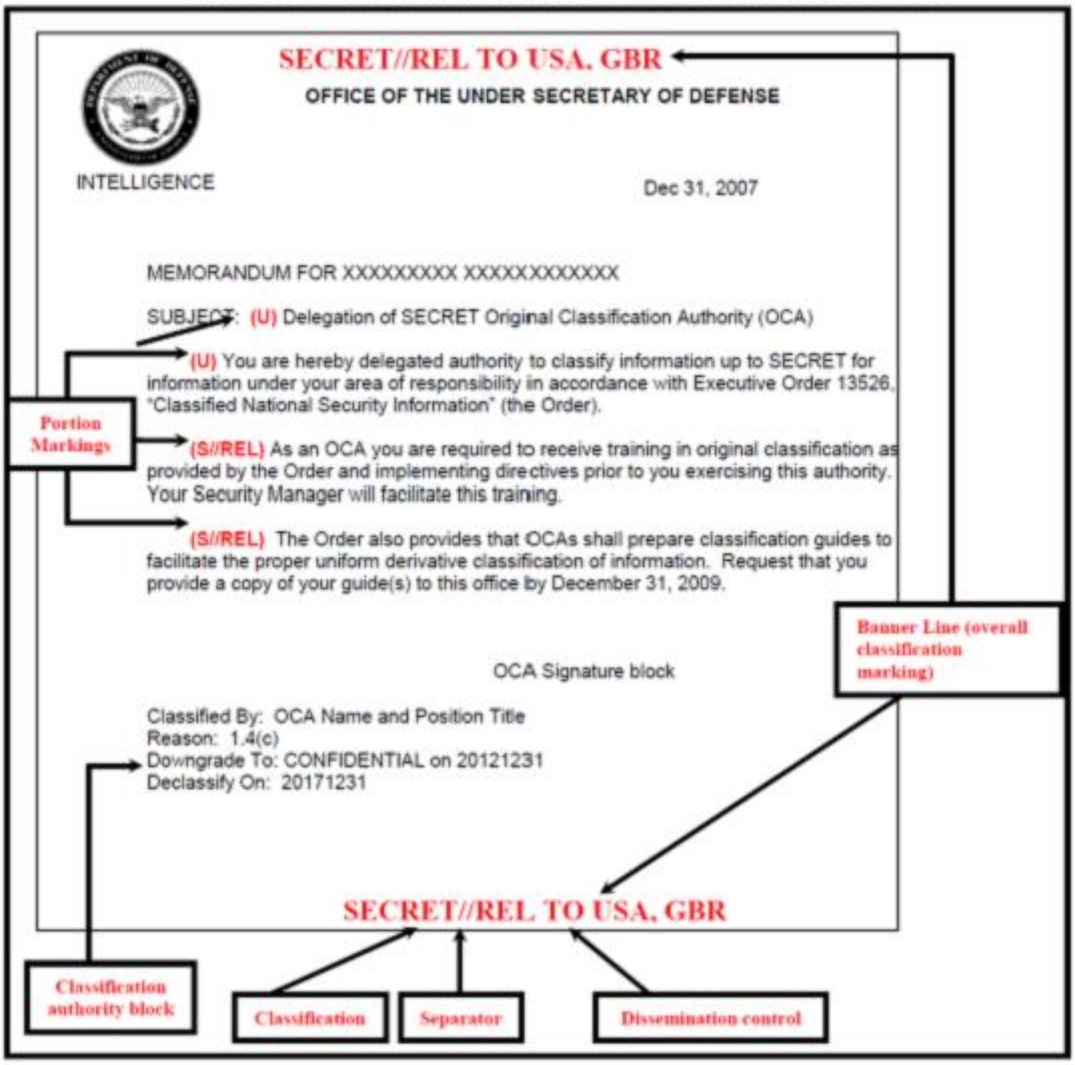
(U)　(C)　(S)　(TS)　(U//FOUO)　(S//NF/PROPIN)

(C//FRD)　(//GBR S)　(TS//SI/TK//RELIDO)　(S//RD)

(S//REL)　(TS//REL TO USA, AUS, CAN, GBR)　(S//RD-N)

Figure 3. Example of Originally Classified Document

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



SECRET//REL TO USA, GBR

OFFICE OF THE UNDER SECRETARY OF DEFENSE

INTELLIGENCE

Dec 31, 2007

MEMORANDUM FOR XXXXXXXXX XXXXXXXXXXXX

SUBJECT: (U) Delegation of SECRET Original Classification Authority (OCA)

(U) You are hereby delegated authority to classify information up to SECRET for information under your area of responsibility in accordance with Executive Order 13526, "Classified National Security Information" (the Order).

(S//REL) As an OCA you are required to receive training in original classification as provided by the Order and implementing directives prior to you exercising this authority. Your Security Manager will facilitate this training.

(S//REL) The Order also provides that OCAs shall prepare classification guides to facilitate the proper uniform derivative classification of information. Request that you provide a copy of your guide(s) to this office by December 31, 2009.

OCA Signature block

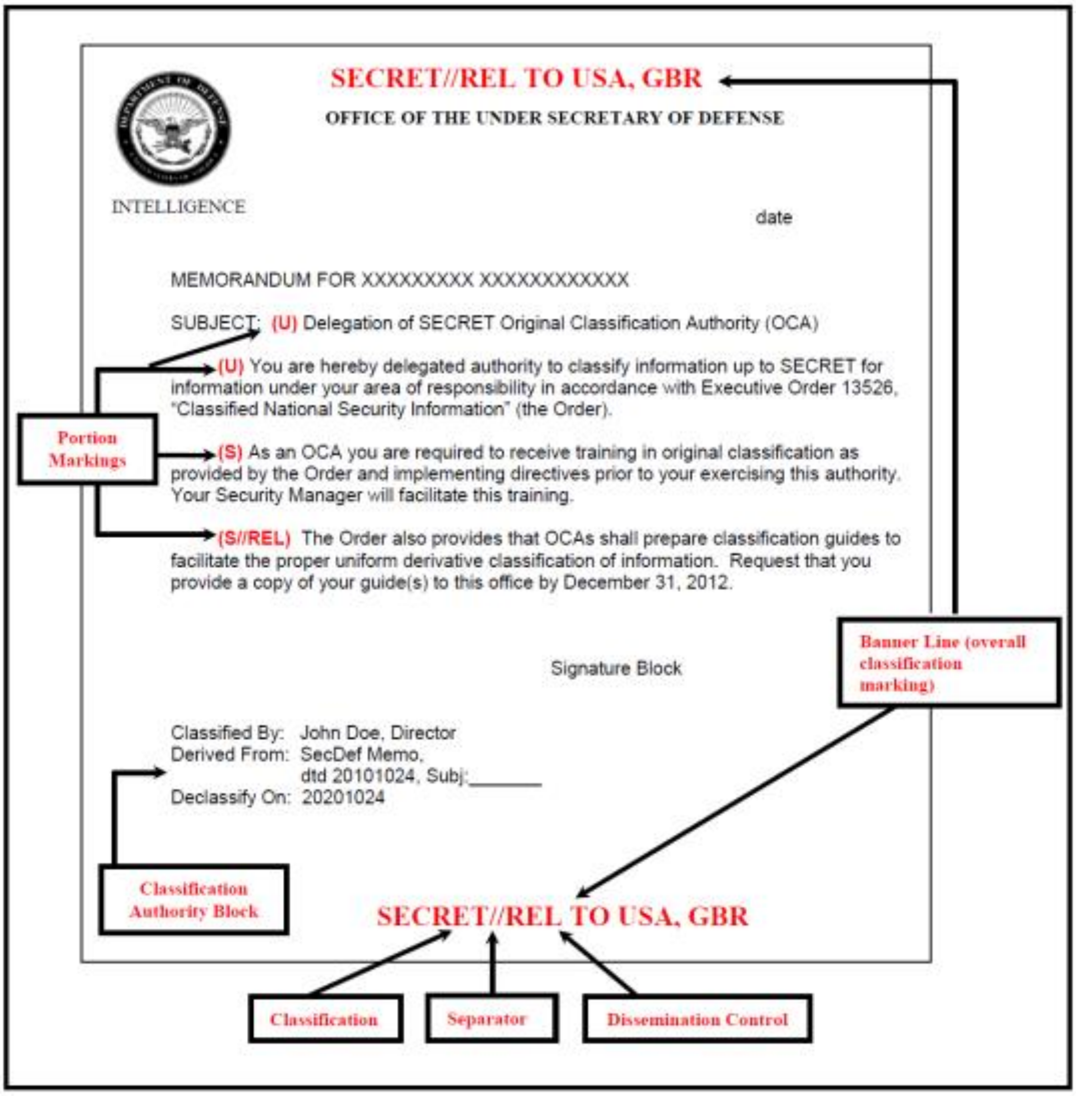
Classified By: OCA Name and Position Title
Reason: 1.4(c)
Downgrade To: CONFIDENTIAL on 20121231
Declassify On: 20171231

SECRET//REL TO USA, GBR

Portion Markings
Banner Line (overall classification marking)
Classification authority block
Classification
Separator
Dissemination control

Figure 4. Example of Derivatively Classified Document

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



SECRET//REL TO USA, GBR

OFFICE OF THE UNDER SECRETARY OF DEFENSE

INTELLIGENCE

date

MEMORANDUM FOR XXXXXXXXX XXXXXXXXXXXX

SUBJECT: (U) Delegation of SECRET Original Classification Authority (OCA)

(U) You are hereby delegated authority to classify information up to SECRET for information under your area of responsibility in accordance with Executive Order 13526, "Classified National Security Information" (the Order).

(S) As an OCA you are required to receive training in original classification as provided by the Order and implementing directives prior to your exercising this authority. Your Security Manager will facilitate this training.

(S//REL) The Order also provides that OCAs shall prepare classification guides to facilitate the proper uniform derivative classification of information. Request that you provide a copy of your guide(s) to this office by December 31, 2012.

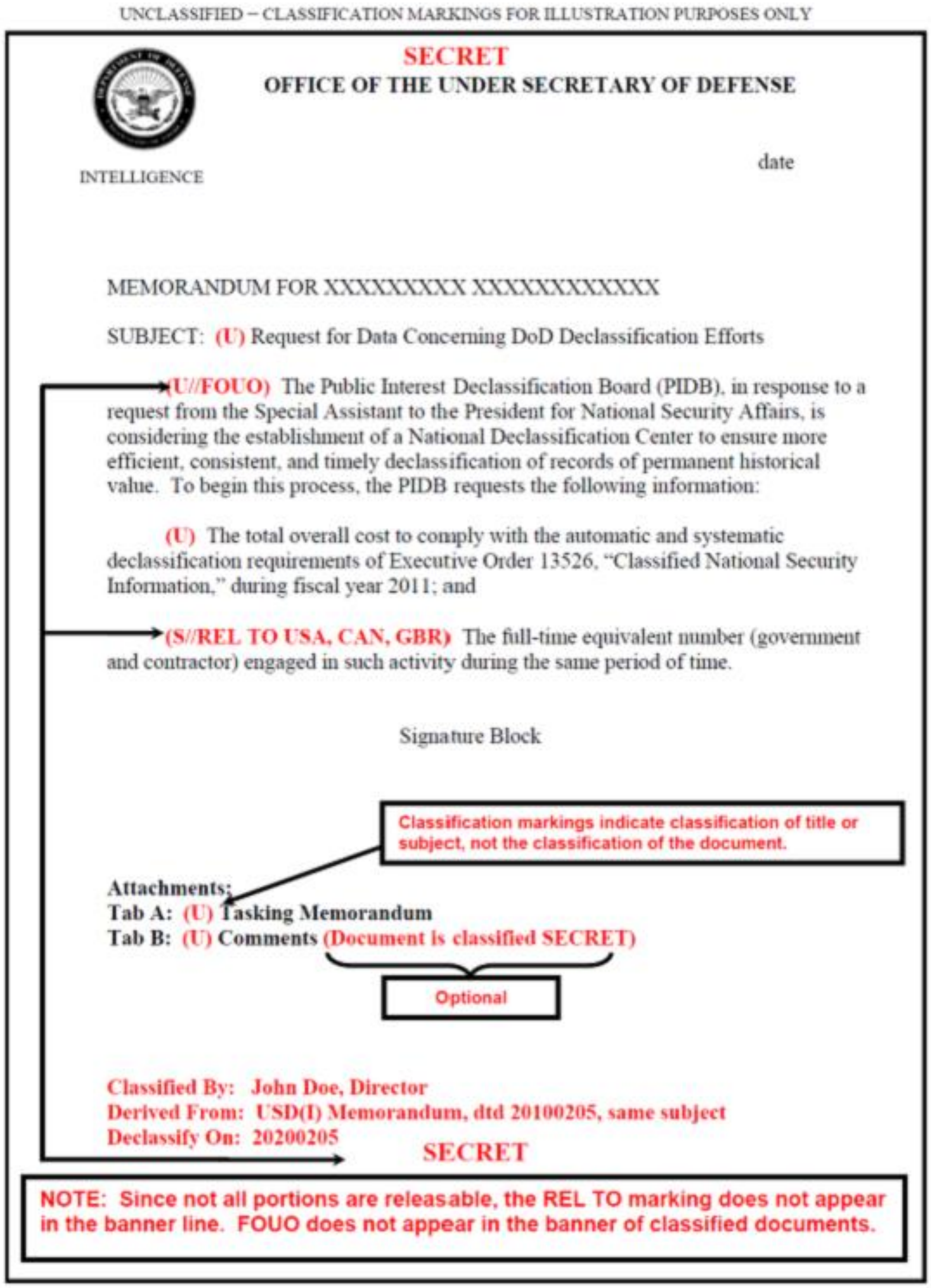
Signature Block

Classified By: John Doe, Director
Derived From: SecDef Memo,
dtd 20101024, Subj:_______
Declassify On: 20201024

SECRET//REL TO USA, GBR

Portion Markings
Banner Line (overall classification marking)
Classification Authority Block
Classification
Separator
Dissemination Control

Figure 5. Markings on a Memorandum



UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

SECRET

OFFICE OF THE UNDER SECRETARY OF DEFENSE

INTELLIGENCE

date

MEMORANDUM FOR XXXXXXXXX XXXXXXXXXXX

SUBJECT: (U) Request for Data Concerning DoD Declassification Efforts

(U//FOUO) The Public Interest Declassification Board (PIDB), in response to a request from the Special Assistant to the President for National Security Affairs, is considering the establishment of a National Declassification Center to ensure more efficient, consistent, and timely declassification of records of permanent historical value. To begin this process, the PIDB requests the following information:

(U) The total overall cost to comply with the automatic and systematic declassification requirements of Executive Order 13526, "Classified National Security Information," during fiscal year 2011; and

(S//REL TO USA, CAN, GBR) The full-time equivalent number (government and contractor) engaged in such activity during the same period of time.

Signature Block

Classification markings indicate classification of title or subject, not the classification of the document.

Attachments:
Tab A: (U) Tasking Memorandum
Tab B: (U) Comments (Document is classified SECRET)

Optional

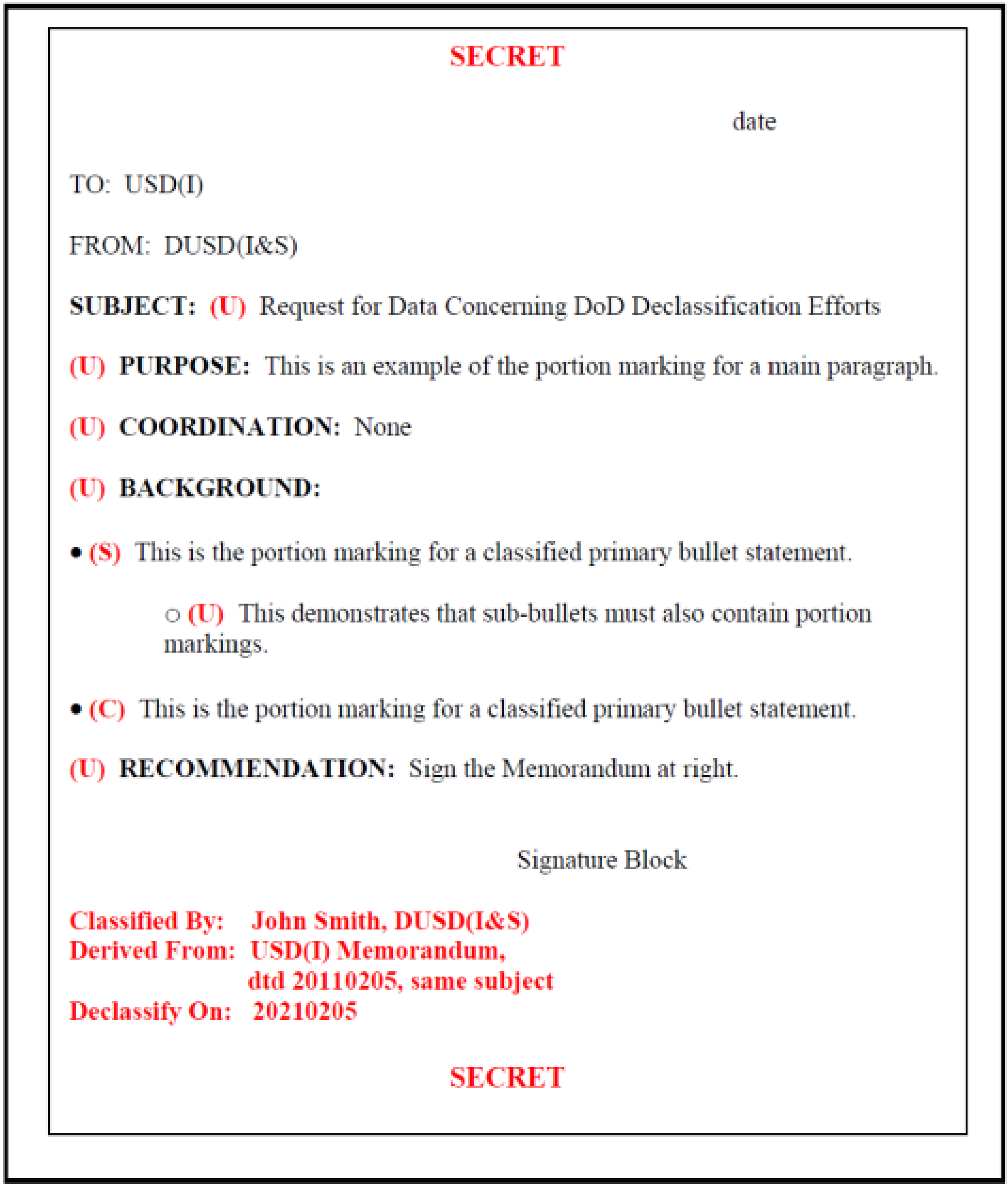
Classified By: John Doe, Director
Derived From: USD(I) Memorandum, dtd 20100205, same subject
Declassify On: 20200205

SECRET

NOTE: Since not all portions are releasable, the REL TO marking does not appear in the banner line. FOUO does not appear in the banner of classified documents.

Figure 6. Markings on an Action Memorandum

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



SECRET

date

TO: USD(I)

FROM: DUSD(I&S)

SUBJECT: (U) Request for Data Concerning DoD Declassification Efforts

(U) **PURPOSE:** This is an example of the portion marking for a main paragraph.

(U) **COORDINATION:** None

(U) **BACKGROUND:**

- (S) This is the portion marking for a classified primary bullet statement.
  - ○ (U) This demonstrates that sub-bullets must also contain portion markings.
- (C) This is the portion marking for a classified primary bullet statement.

(U) **RECOMMENDATION:** Sign the Memorandum at right.

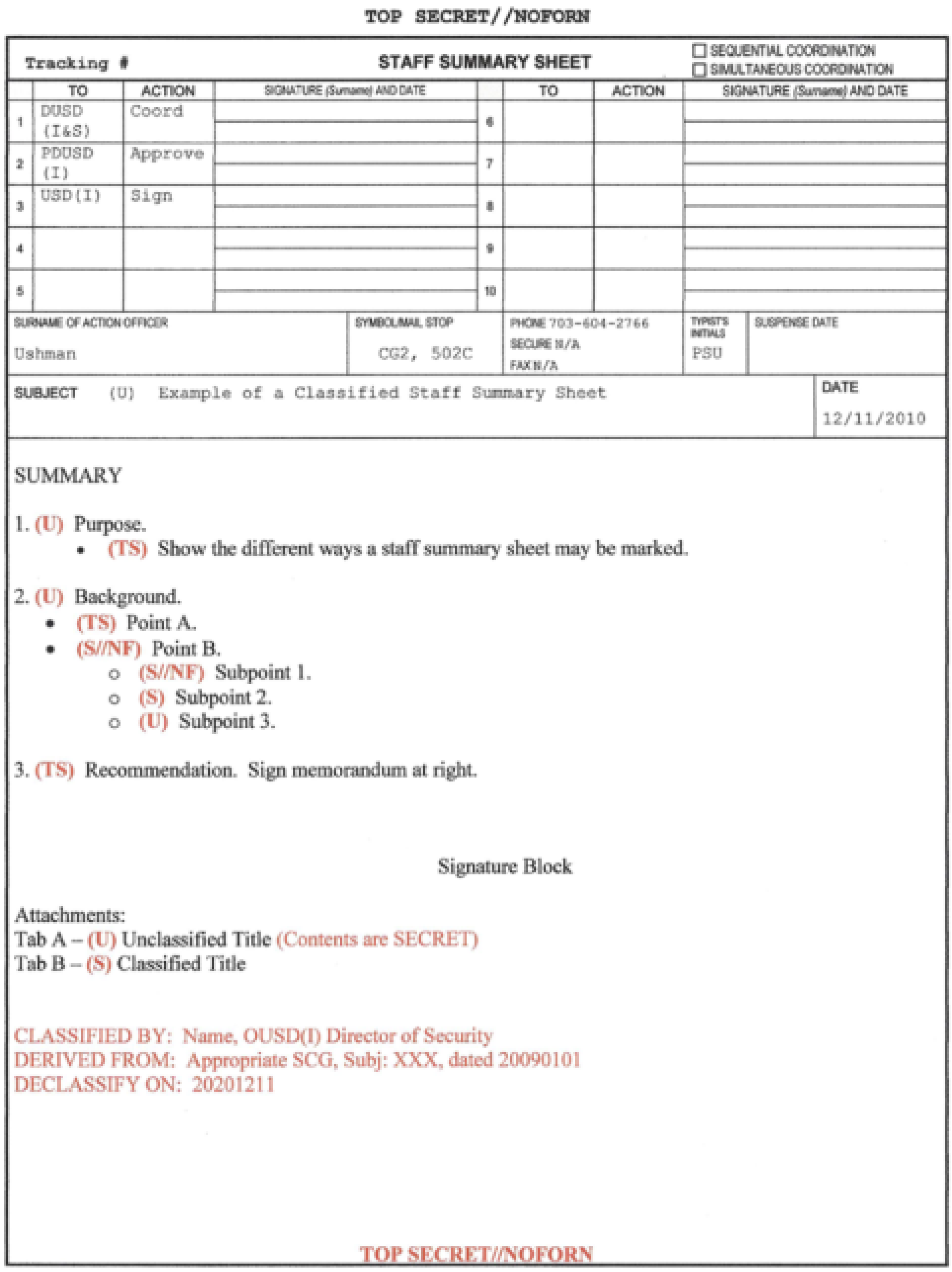
Signature Block

Classified By: John Smith, DUSD(I&S)
Derived From: USD(I) Memorandum,
dtd 20110205, same subject
Declassify On: 20210205

SECRET

Figure 7. Markings on a Staff Summary Sheet

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



TOP SECRET//NOFORN

Tracking #		STAFF SUMMARY SHEET				□ SEQUENTIAL COORDINATION □ SIMULTANEOUS COORDINATION
	TO	ACTION	SIGNATURE (Surname) AND DATE		TO	ACTION	SIGNATURE (Surname) AND DATE

	TO	ACTION	SIGNATURE (Surname) AND DATE		TO	ACTION	SIGNATURE (Surname) AND DATE
1	DUSD (I&S)	Coord		6			
2	PDUSD (I)	Approve		7			
3	USD(I)	Sign		8			
4				9			
5				10			

SURNAME OF ACTION OFFICER	SYMBOL/MAIL STOP	PHONE 703-604-2766 SECURE N/A FAX N/A	TYPIST'S INITIALS	SUSPENSE DATE
Ushman	CG2, 502C		PSU	

SUBJECT (U) Example of a Classified Staff Summary Sheet

DATE 12/11/2010

SUMMARY

1. (U) Purpose.
    - (TS) Show the different ways a staff summary sheet may be marked.

2. (U) Background.
    - (TS) Point A.
    - (S//NF) Point B.
        - (S//NF) Subpoint 1.
        - (S) Subpoint 2.
        - (U) Subpoint 3.

3. (TS) Recommendation. Sign memorandum at right.

Signature Block

Attachments:
Tab A – (U) Unclassified Title (Contents are SECRET)
Tab B – (S) Classified Title

CLASSIFIED BY: Name, OUSD(I) Director of Security
DERIVED FROM: Appropriate SCG, Subj: XXX, dated 20090101
DECLASSIFY ON: 20201211

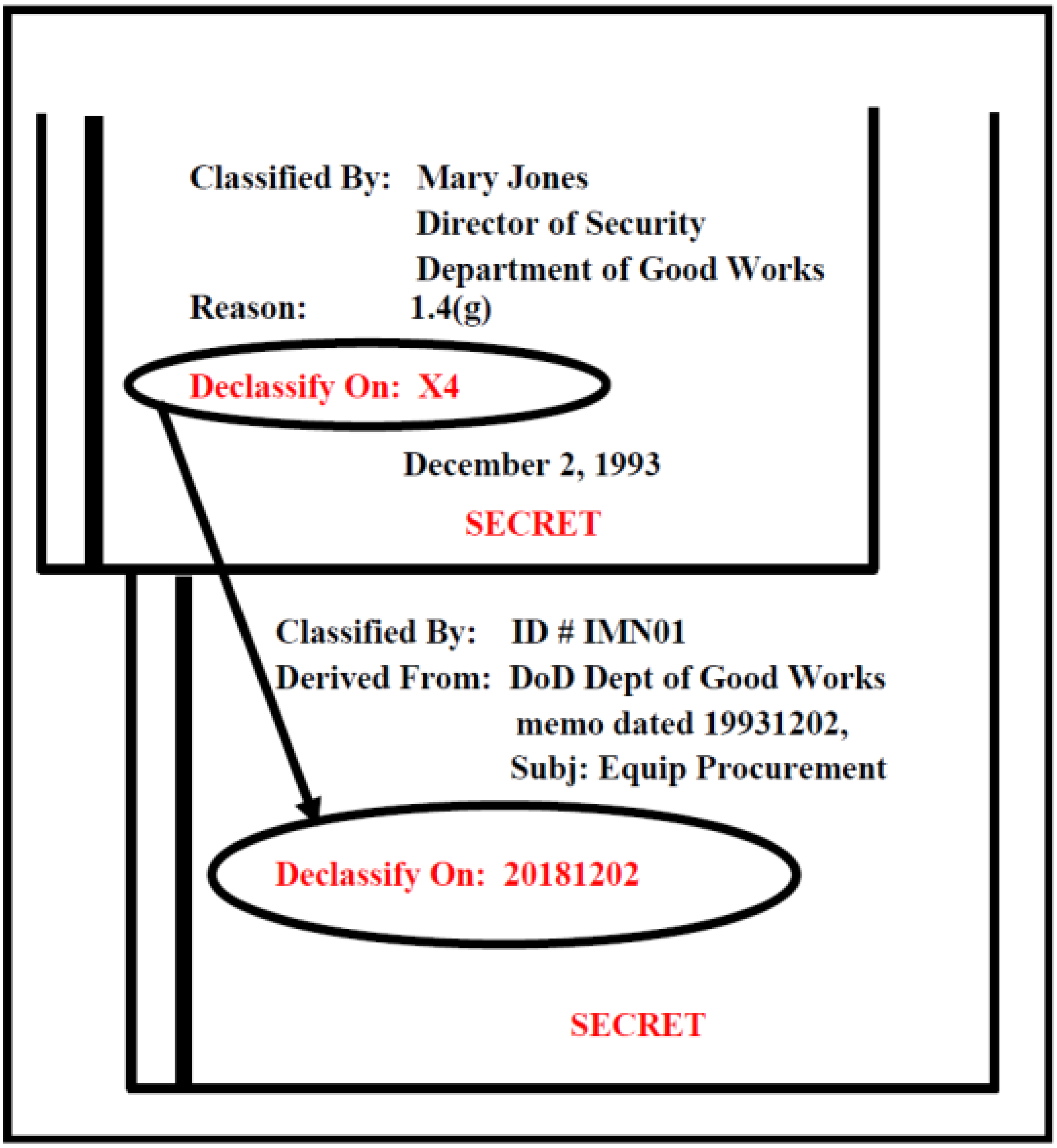
TOP SECRET//NOFORN

Example shows markings for paragraphs and subparagraphs, including those beginning with bullets.

The banner line shows the highest classification in the document (TOP SECRET) and also includes the dissemination control marking NOFORN, as it is included among the portion markings for specific information.

Figure 8. Use of Calculated Declassification Date

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



Classified By: Mary Jones
Director of Security
Department of Good Works
Reason: 1.4(g)

Declassify On: X4

December 2, 1993

SECRET

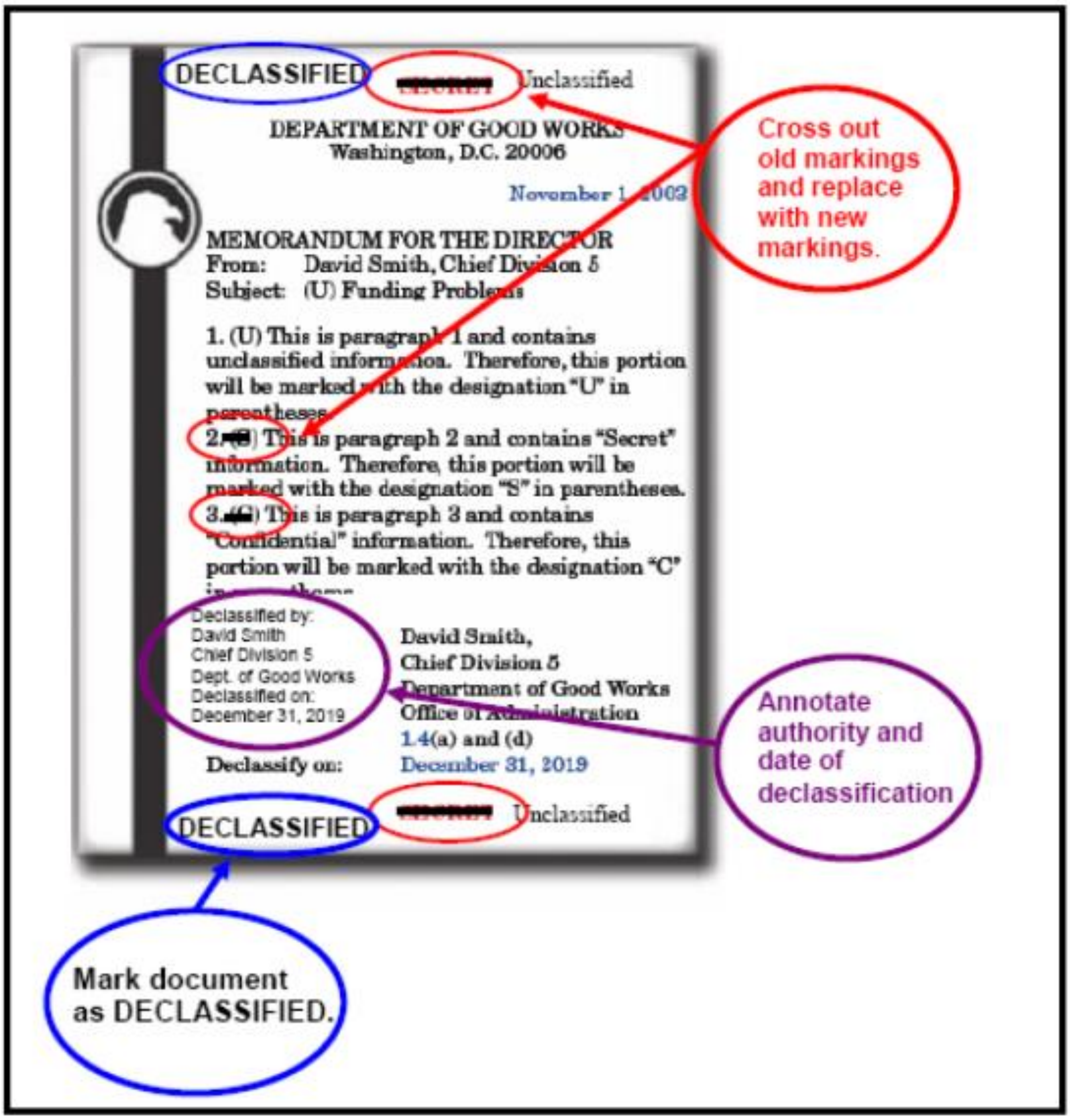
Classified By: ID # IMN01
Derived From: DoD Dept of Good Works
memo dated 19931202,
Subj: Equip Procurement

Declassify On: 20181202

SECRET

Figure 9. Declassification Markings

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



DECLASSIFIED ~~SECRET~~ Unclassified

DEPARTMENT OF GOOD WORKS
Washington, D.C. 20006

November 1, 2003

MEMORANDUM FOR THE DIRECTOR
From: David Smith, Chief Division 5
Subject: (U) Funding Problems

1. (U) This is paragraph 1 and contains unclassified information. Therefore, this portion will be marked with the designation "U" in parentheses.

2. ~~(S)~~ This is paragraph 2 and contains "Secret" information. Therefore, this portion will be marked with the designation "S" in parentheses.

3. ~~(C)~~ This is paragraph 3 and contains "Confidential" information. Therefore, this portion will be marked with the designation "C" in parentheses.

Declassified by:
David Smith
Chief Division 5
Dept. of Good Works
Declassified on:
December 31, 2019

David Smith,
Chief Division 5
Department of Good Works
Office of Administration
1.4(a) and (d)

Declassify on: December 31, 2019

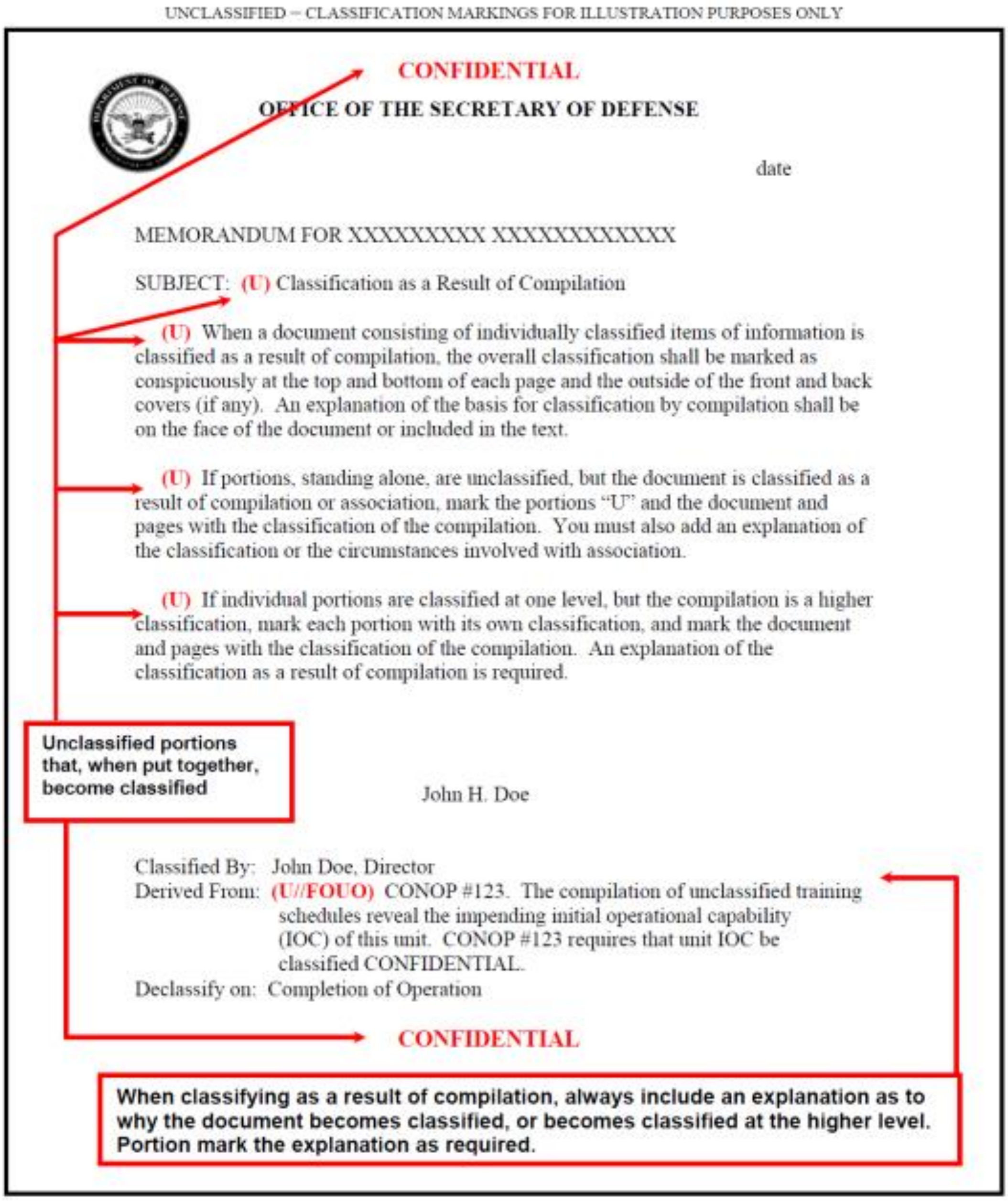
DECLASSIFIED ~~SECRET~~ Unclassified

Cross out old markings and replace with new markings.

Annotate authority and date of declassification

Mark document as DECLASSIFIED.

Figure 10. Classification as a Result of Compilation



UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

CONFIDENTIAL

OFFICE OF THE SECRETARY OF DEFENSE

date

MEMORANDUM FOR XXXXXXXXX XXXXXXXXXXXX

SUBJECT: (U) Classification as a Result of Compilation

(U) When a document consisting of individually classified items of information is classified as a result of compilation, the overall classification shall be marked as conspicuously at the top and bottom of each page and the outside of the front and back covers (if any). An explanation of the basis for classification by compilation shall be on the face of the document or included in the text.

(U) If portions, standing alone, are unclassified, but the document is classified as a result of compilation or association, mark the portions "U" and the document and pages with the classification of the compilation. You must also add an explanation of the classification or the circumstances involved with association.

(U) If individual portions are classified at one level, but the compilation is a higher classification, mark each portion with its own classification, and mark the document and pages with the classification of the compilation. An explanation of the classification as a result of compilation is required.

Unclassified portions that, when put together, become classified

John H. Doe

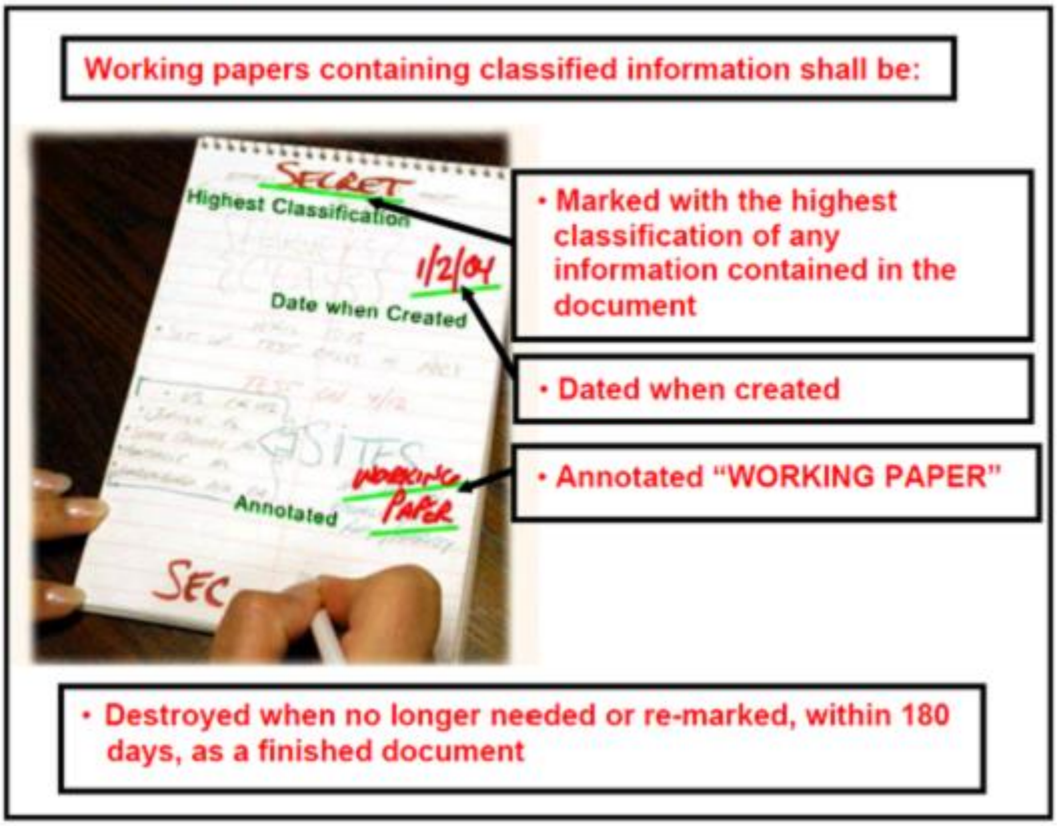
Classified By: John Doe, Director
Derived From: (U//FOUO) CONOP #123. The compilation of unclassified training schedules reveal the impending initial operational capability (IOC) of this unit. CONOP #123 requires that unit IOC be classified CONFIDENTIAL.
Declassify on: Completion of Operation

CONFIDENTIAL

When classifying as a result of compilation, always include an explanation as to why the document becomes classified, or becomes classified at the higher level. Portion mark the explanation as required.

Figure 11. Markings on Working Papers

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY


SECRET
Highest Classification
1/2/04
Date when Created
WORKING PAPER
Annotated
SEC

Working papers containing classified information shall be:

- Marked with the highest classification of any information contained in the document
- Dated when created
- Annotated "WORKING PAPER"
- Destroyed when no longer needed or re-marked, within 180 days, as a finished document

Figure 12. Marking References

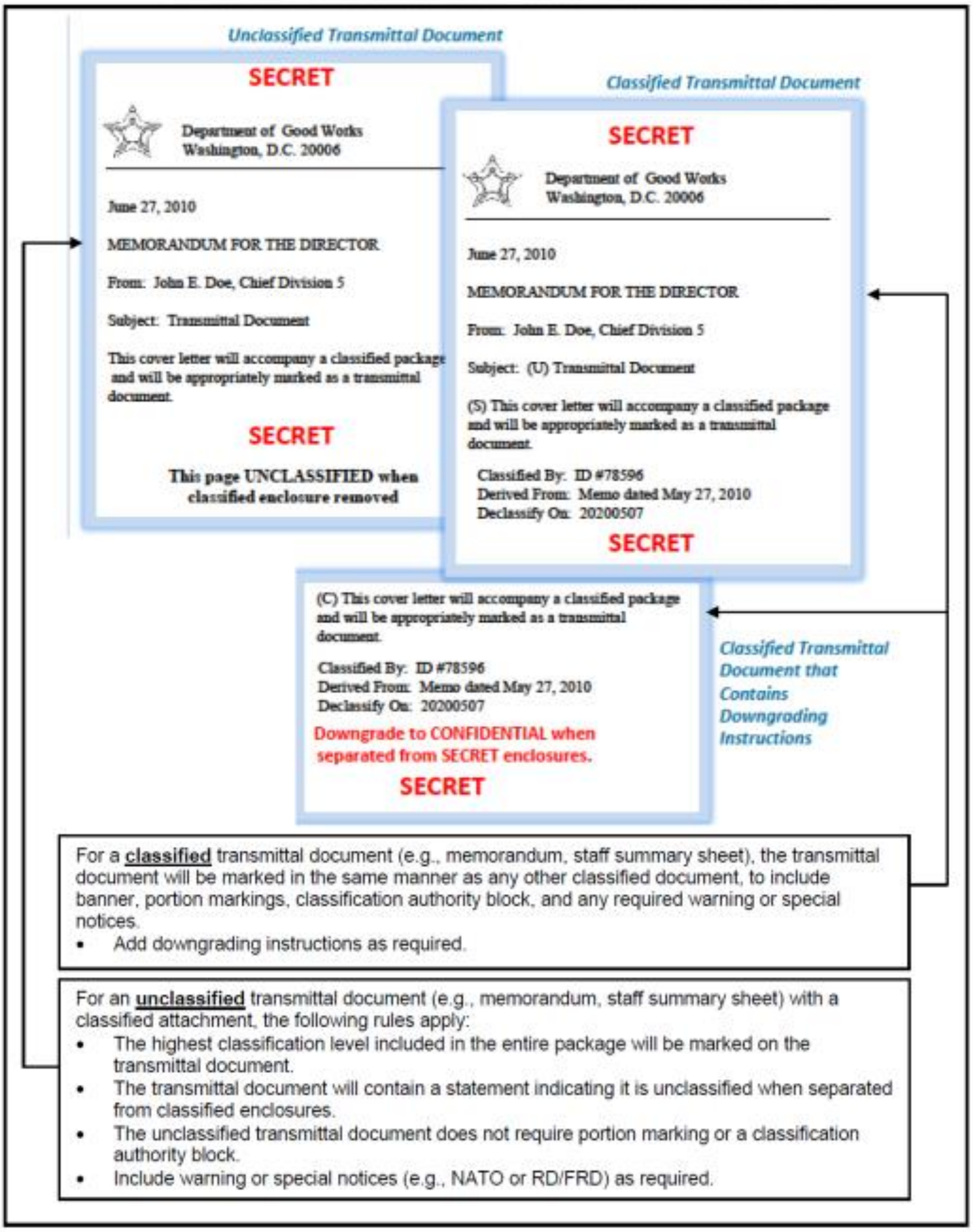
UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

(U) Executive Order 13526, "Classified National Security Information," December 29, 2009

(U) Under Secretary of Defense for Intelligence (USD(I)) Memorandum, "Security Classification Marking Instructions," September 27, 2004 (Document is classified Secret.)

Figure 13. Transmittal Documents

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



Unclassified Transmittal Document

SECRET

Department of Good Works
Washington, D.C. 20006

June 27, 2010

MEMORANDUM FOR THE DIRECTOR

From: John E. Doe, Chief Division 5

Subject: Transmittal Document

This cover letter will accompany a classified package and will be appropriately marked as a transmittal document.

SECRET

This page UNCLASSIFIED when classified enclosure removed

Classified Transmittal Document

SECRET

Department of Good Works
Washington, D.C. 20006

June 27, 2010

MEMORANDUM FOR THE DIRECTOR

From: John E. Doe, Chief Division 5

Subject: (U) Transmittal Document

(S) This cover letter will accompany a classified package and will be appropriately marked as a transmittal document.

Classified By: ID #78596
Derived From: Memo dated May 27, 2010
Declassify On: 20200507

SECRET

(C) This cover letter will accompany a classified package and will be appropriately marked as a transmittal document.

Classified By: ID #78596
Derived From: Memo dated May 27, 2010
Declassify On: 20200507

Downgrade to CONFIDENTIAL when separated from SECRET enclosures.

SECRET

Classified Transmittal Document that Contains Downgrading Instructions

For a **classified** transmittal document (e.g., memorandum, staff summary sheet), the transmittal document will be marked in the same manner as any other classified document, to include banner, portion markings, classification authority block, and any required warning or special notices.

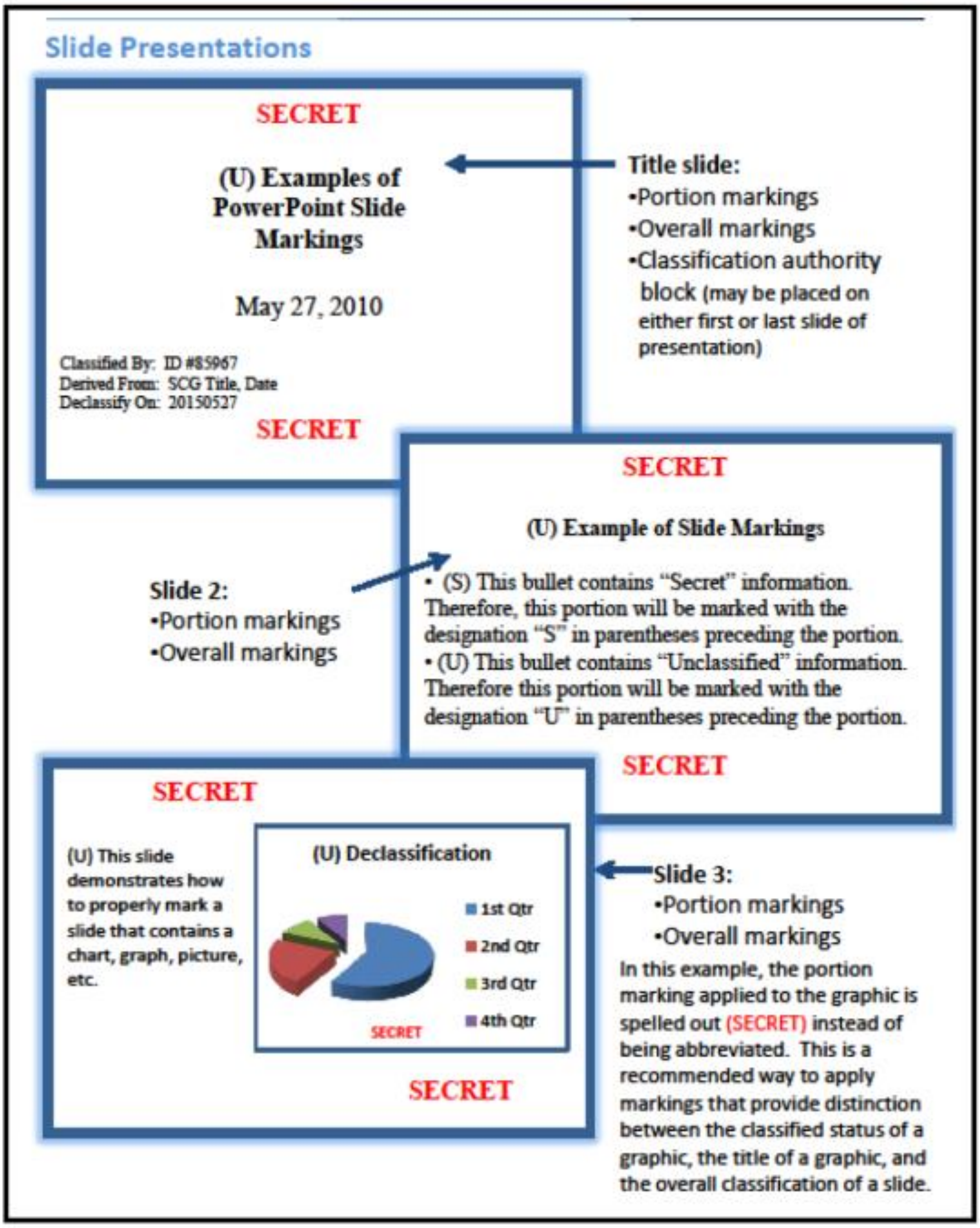
- Add downgrading instructions as required.

For an **unclassified** transmittal document (e.g., memorandum, staff summary sheet) with a classified attachment, the following rules apply:

- The highest classification level included in the entire package will be marked on the transmittal document.
- The transmittal document will contain a statement indicating it is unclassified when separated from classified enclosures.
- The unclassified transmittal document does not require portion marking or a classification authority block.
- Include warning or special notices (e.g., NATO or RD/FRD) as required.

Figure 14. Markings on Briefing Slides

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



Slide Presentations

SECRET

(U) Examples of PowerPoint Slide Markings

May 27, 2010

Classified By: ID #85967
Derived From: SCG Title, Date
Declassify On: 20150527

SECRET

Title slide:
- •Portion markings
- •Overall markings
- •Classification authority block (may be placed on either first or last slide of presentation)

SECRET

(U) Example of Slide Markings

- • (S) This bullet contains "Secret" information. Therefore, this portion will be marked with the designation "S" in parentheses preceding the portion.
- • (U) This bullet contains "Unclassified" information. Therefore this portion will be marked with the designation "U" in parentheses preceding the portion.

SECRET

Slide 2:
- •Portion markings
- •Overall markings

SECRET

(U) This slide demonstrates how to properly mark a slide that contains a chart, graph, picture, etc.

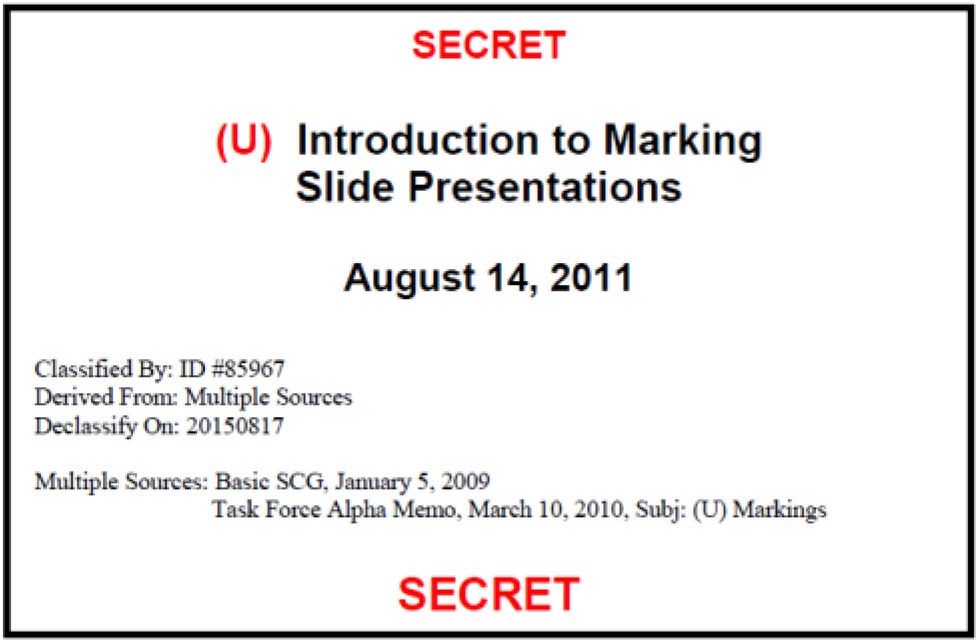
SECRET

Slide 3:
- •Portion markings
- •Overall markings

In this example, the portion marking applied to the graphic is spelled out (SECRET) instead of being abbreviated. This is a recommended way to apply markings that provide distinction between the classified status of a graphic, the title of a graphic, and the overall classification of a slide.

Figure 15. Multiple Source Listing on Briefing Slides

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



SECRET

(U) Introduction to Marking
Slide Presentations

August 14, 2011

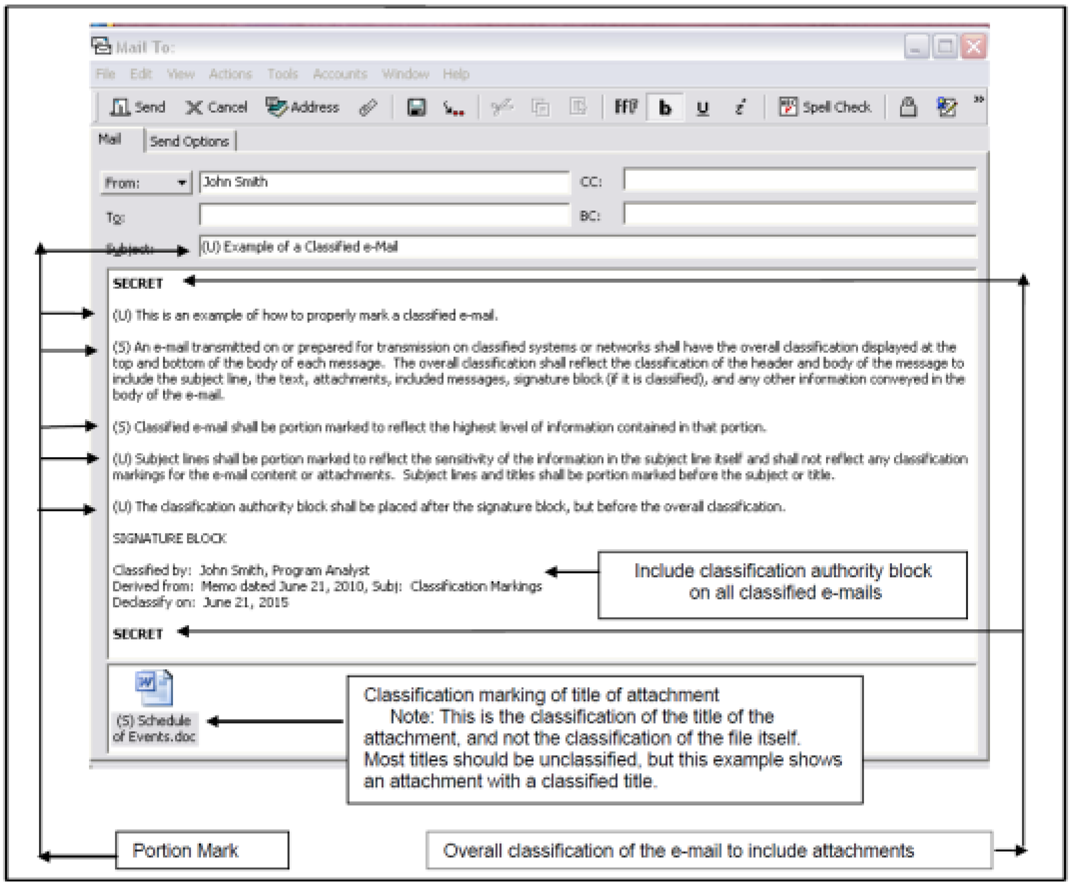
Classified By: ID #85967
Derived From: Multiple Sources
Declassify On: 20150817

Multiple Sources: Basic SCG, January 5, 2009
Task Force Alpha Memo, March 10, 2010, Subj: (U) Markings

SECRET

Figure 16. Marking E-Mails

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



John Smith

(U) Example of a Classified e-Mail

SECRET

(U) This is an example of how to properly mark a classified e-mail.

(S) An e-mail transmitted on or prepared for transmission on classified systems or networks shall have the overall classification displayed at the top and bottom of the body of each message. The overall classification shall reflect the classification of the header and body of the message to include the subject line, the text, attachments, included messages, signature block (if it is classified), and any other information conveyed in the body of the e-mail.

(S) Classified e-mail shall be portion marked to reflect the highest level of information contained in that portion.

(U) Subject lines shall be portion marked to reflect the sensitivity of the information in the subject line itself and shall not reflect any classification markings for the e-mail content or attachments. Subject lines and titles shall be portion marked before the subject or title.

(U) The classification authority block shall be placed after the signature block, but before the overall classification.

SIGNATURE BLOCK

Classified by: John Smith, Program Analyst
Derived from: Memo dated June 21, 2010, Subj: Classification Markings
Declassify on: June 21, 2015

SECRET

(S) Schedule of Events.doc

Include classification authority block on all classified e-mails

Classification marking of title of attachment
Note: This is the classification of the title of the attachment, and not the classification of the file itself. Most titles should be unclassified, but this example shows an attachment with a classified title.

Portion Mark

Overall classification of the e-mail to include attachments

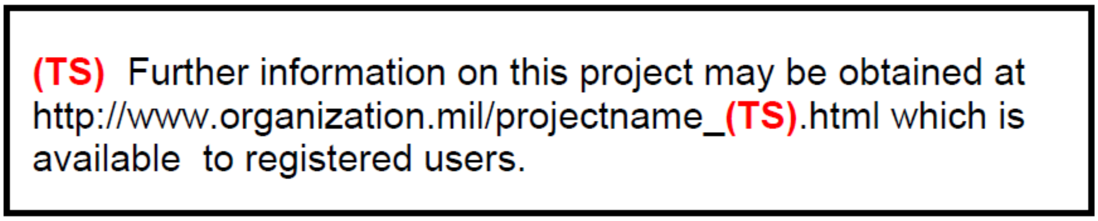
Figure 17. Examples of URL with Included Portion Mark

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

http://www.center.xyz/SECRET/filename_(S).html
http://www.center.xyz/filename2_(TS).html
http://www.center.xyz/filename_(TS//NF).html

Figure 18. Example of Portion-Marked URL Embedded in Text

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



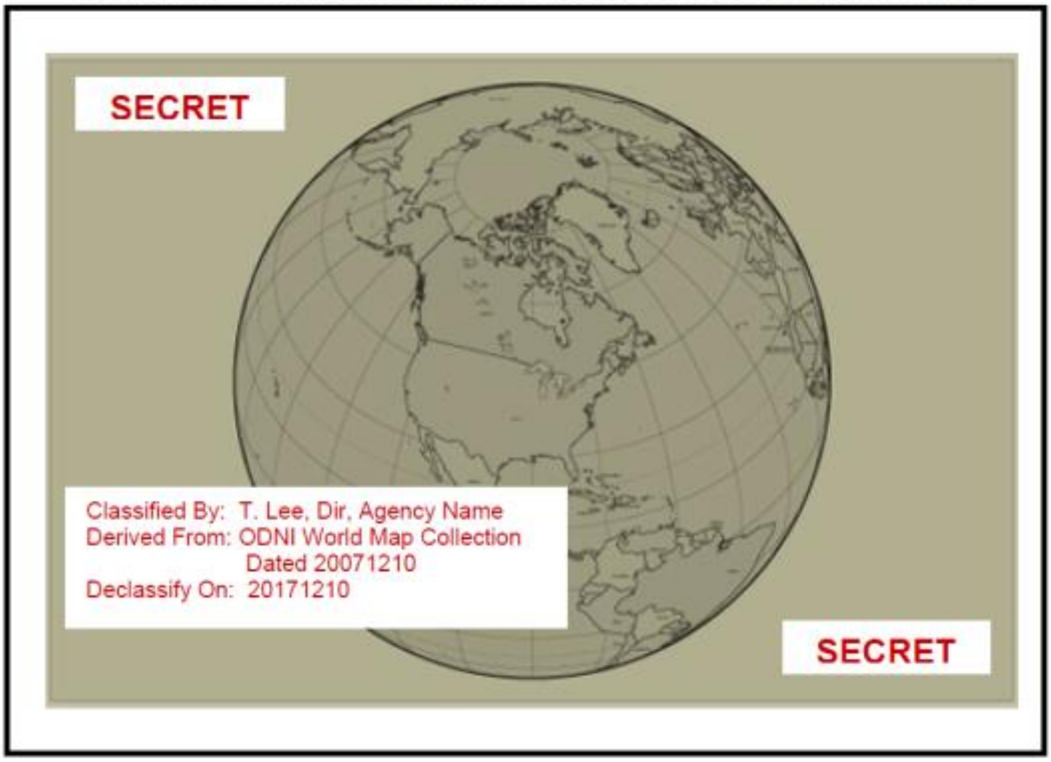
(TS) Further information on this project may be obtained at http://www.organization.mil/projectname_(TS).html which is available to registered users.

Figure 19. Warning Statement for Dynamic Documents

This content is classified at the [insert highest classification level of the source data] level and may contain elements of information that are unclassified or classified at a lower level than the overall classification displayed. This content shall not be used as a source of derivative classification; refer instead to [cite specific reference, where possible, or state "the applicable classification guide(s)"]. [Add a point of contact when needed.]

Figure 20. Markings on Maps

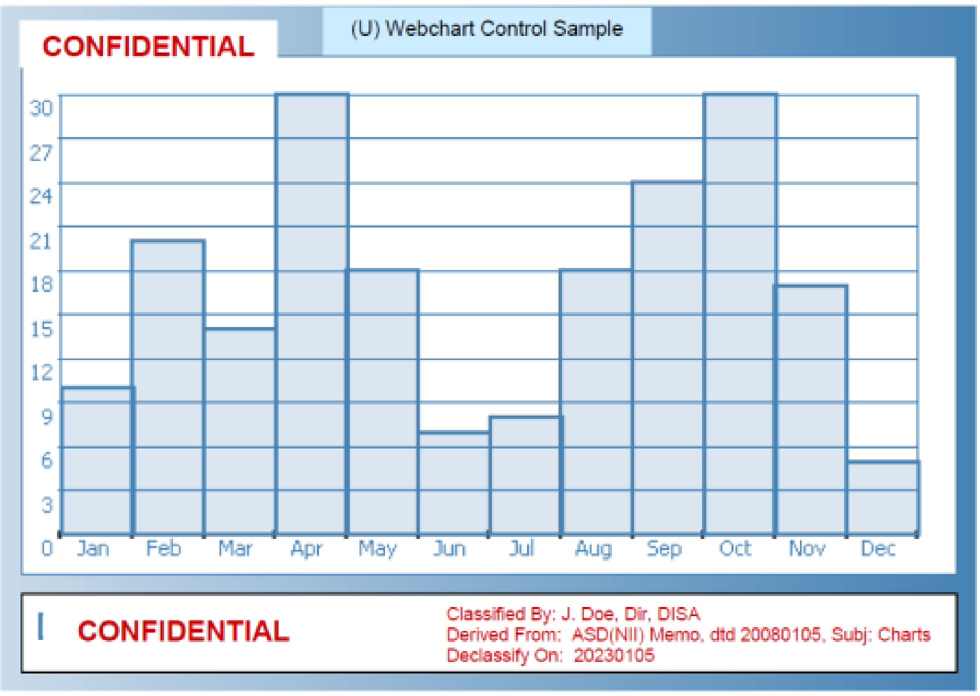
UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



Classified By: T. Lee, Dir, Agency Name
Derived From: ODNI World Map Collection
Dated 20071210
Declassify On: 20171210

Figure 21. Markings on Charts

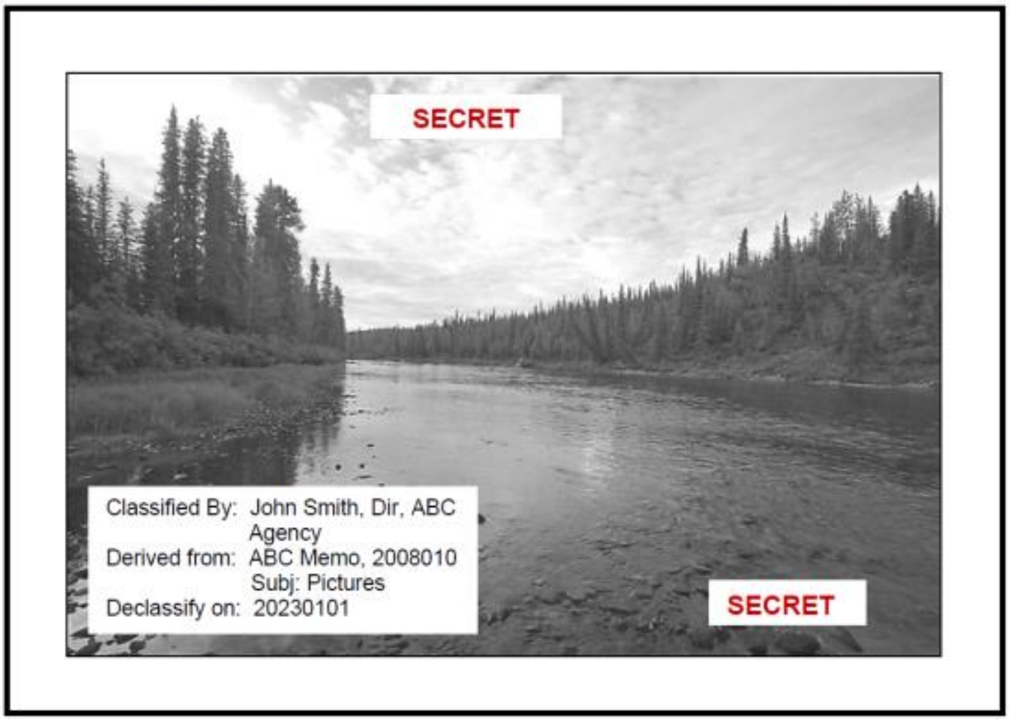
UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



Classified By: J. Doe, Dir, DISA
Derived From: ASD(NII) Memo, dtd 20080105, Subj: Charts
Declassify On: 20230105

Figure 22. Markings on Photographs

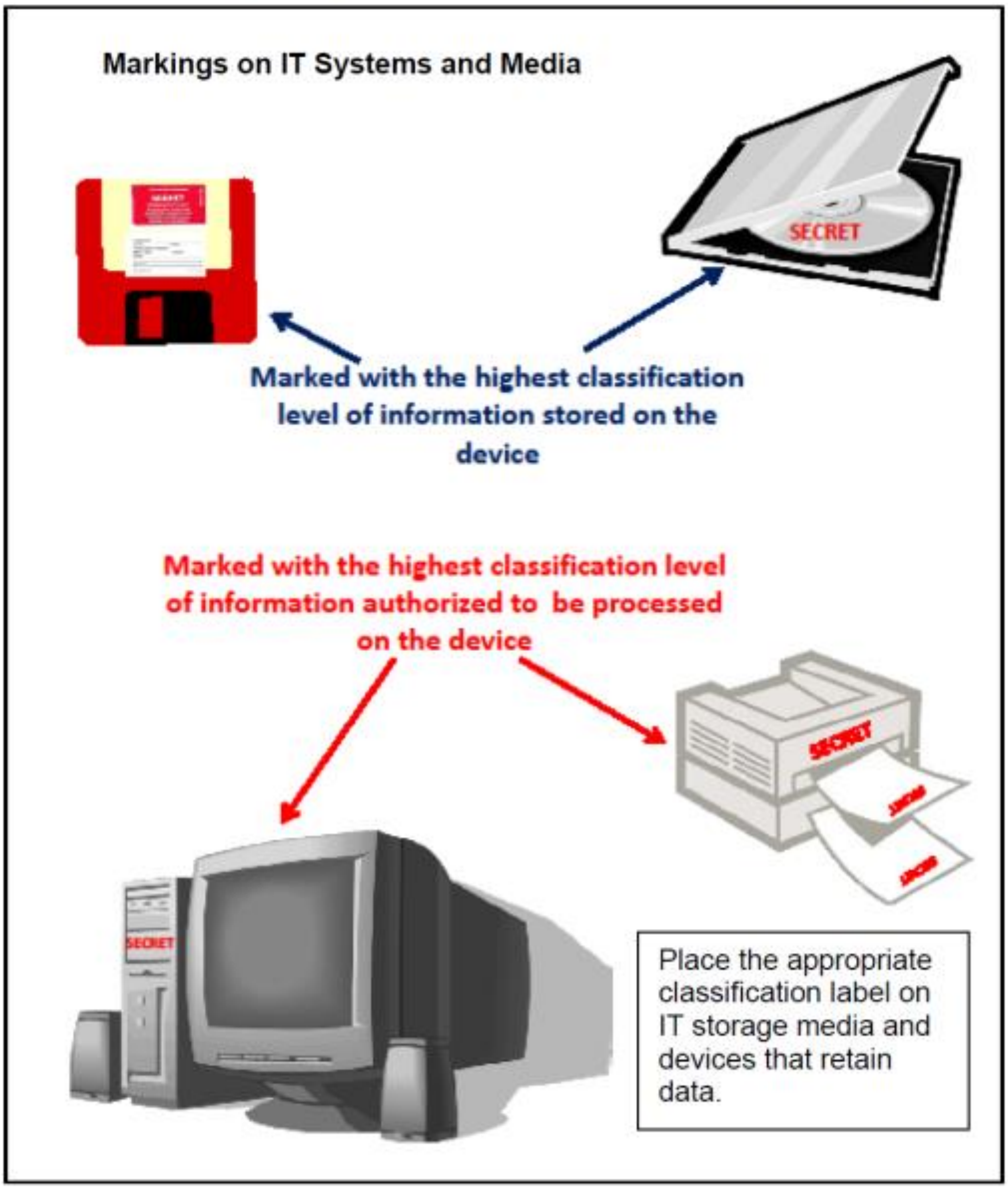
UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



Classified By: John Smith, Dir, ABC Agency
Derived from: ABC Memo, 2008010 Subj: Pictures
Declassify on: 20230101

Figure 23. Markings on IT Systems and Media

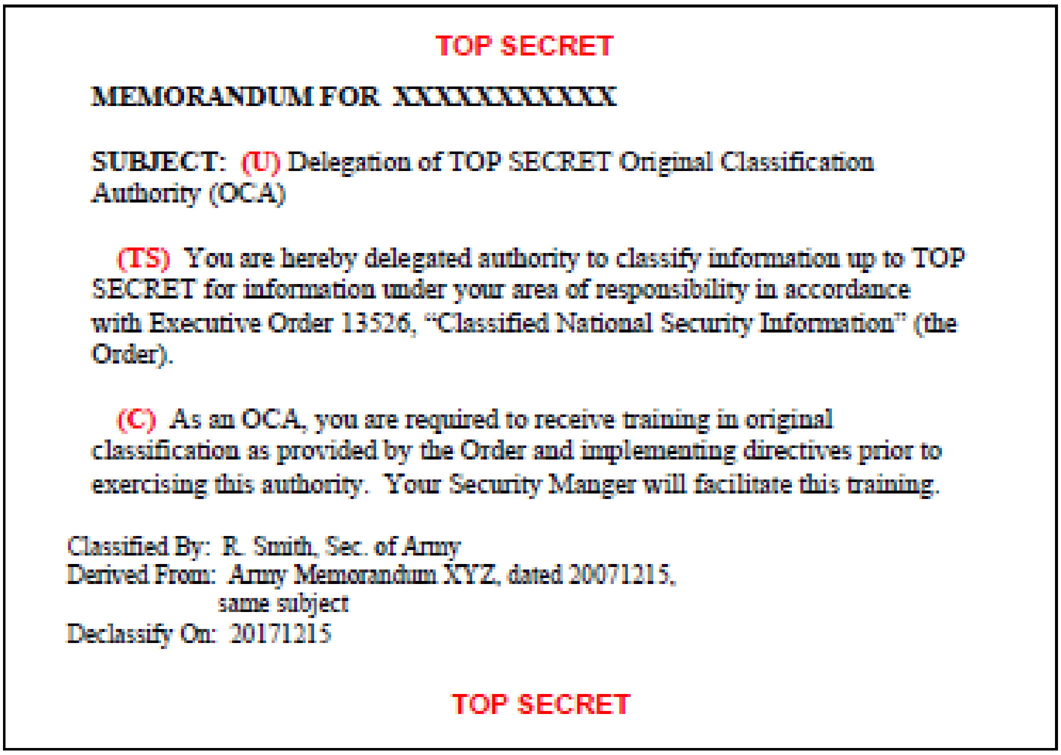
UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



Markings on IT Systems and Media
SECRET
Marked with the highest classification level of information stored on the device
Marked with the highest classification level of information authorized to be processed on the device
SECRET
SECRET
Place the appropriate classification label on IT storage media and devices that retain data.

Figure 26. Example of U.S. Classification Markings

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



TOP SECRET

MEMORANDUM FOR XXXXXXXXXXXX

SUBJECT: (U) Delegation of TOP SECRET Original Classification Authority (OCA)

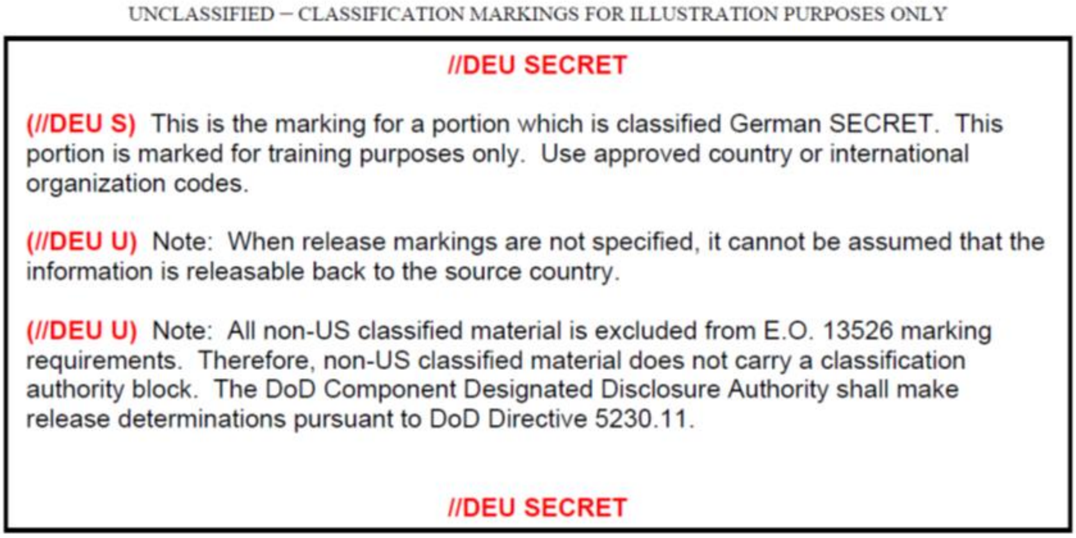
(TS) You are hereby delegated authority to classify information up to TOP SECRET for information under your area of responsibility in accordance with Executive Order 13526, "Classified National Security Information" (the Order).

(C) As an OCA, you are required to receive training in original classification as provided by the Order and implementing directives prior to exercising this authority. Your Security Manger will facilitate this training.

Classified By: R. Smith, Sec. of Army
Derived From: Army Memorandum XYZ, dated 20071215,
same subject
Declassify On: 20171215

TOP SECRET

Figure 27. Example of Markings for Non-U.S. Documents



UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

//DEU SECRET

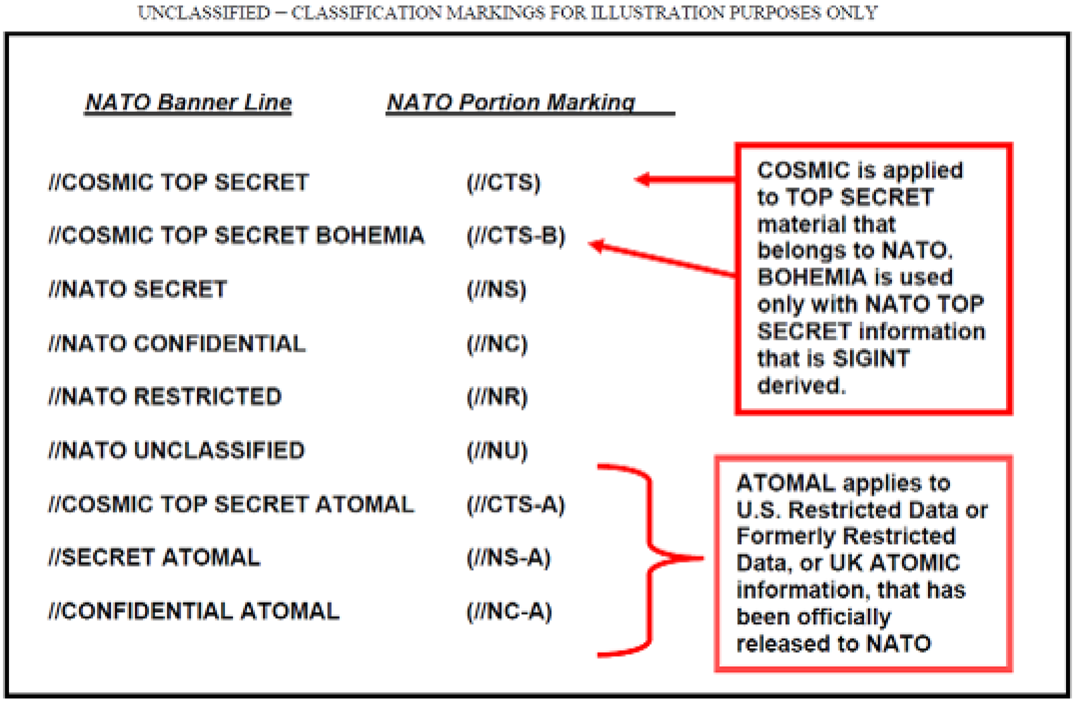
(//DEU S) This is the marking for a portion which is classified German SECRET. This portion is marked for training purposes only. Use approved country or international organization codes.

(//DEU U) Note: When release markings are not specified, it cannot be assumed that the information is releasable back to the source country.

(//DEU U) Note: All non-US classified material is excluded from E.O. 13526 marking requirements. Therefore, non-US classified material does not carry a classification authority block. The DoD Component Designated Disclosure Authority shall make release determinations pursuant to DoD Directive 5230.11.

//DEU SECRET

Figure 28. Examples of NATO Markings



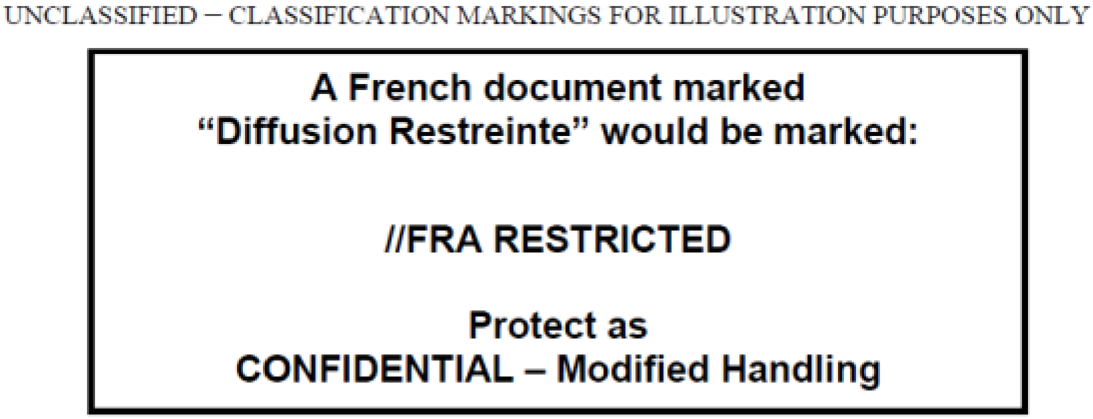
UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

NATO Banner Line	*NATO Portion Marking*
//COSMIC TOP SECRET	(//CTS)
//COSMIC TOP SECRET BOHEMIA	(//CTS-B)
//NATO SECRET	(//NS)
//NATO CONFIDENTIAL	(//NC)
//NATO RESTRICTED	(//NR)
//NATO UNCLASSIFIED	(//NU)
//COSMIC TOP SECRET ATOMAL	(//CTS-A)
//SECRET ATOMAL	(//NS-A)
//CONFIDENTIAL ATOMAL	(//NC-A)

COSMIC is applied to TOP SECRET material that belongs to NATO. BOHEMIA is used only with NATO TOP SECRET information that is SIGINT derived.

ATOMAL applies to U.S. Restricted Data or Formerly Restricted Data, or UK ATOMIC information, that has been officially released to NATO

Figure 29. CONFIDENTIAL-Modified Handling Example



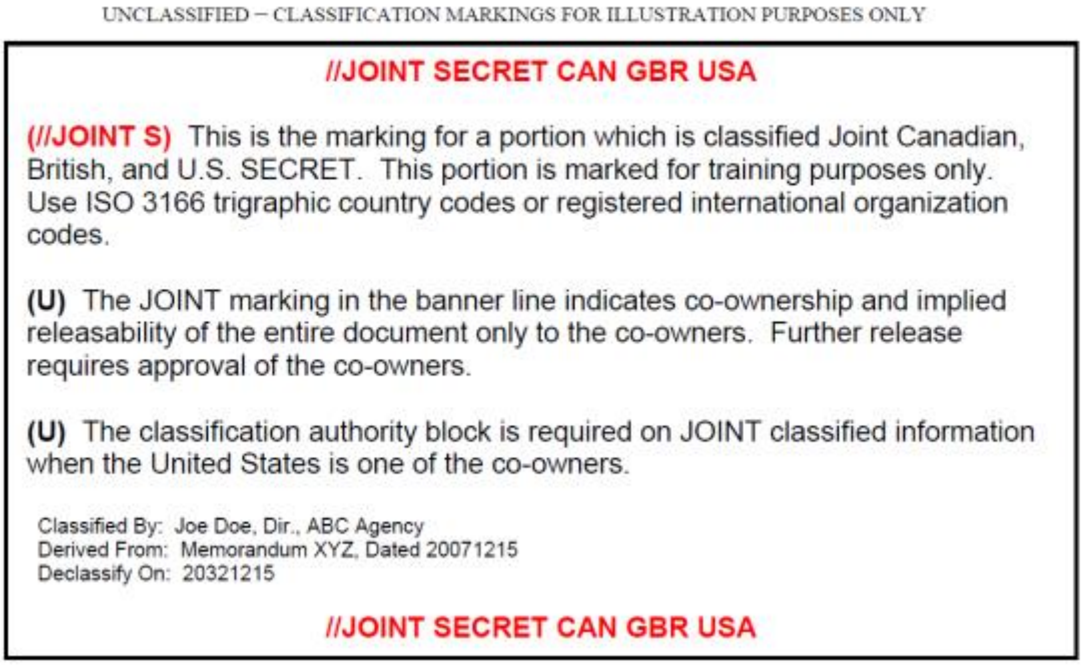
UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

A French document marked
“Diffusion Restreinte” would be marked:

//FRA RESTRICTED

Protect as
CONFIDENTIAL – Modified Handling

Figure 30. Example of Joint Classification Marking



UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

//JOINT SECRET CAN GBR USA

(//JOINT S) This is the marking for a portion which is classified Joint Canadian, British, and U.S. SECRET. This portion is marked for training purposes only. Use ISO 3166 trigraphic country codes or registered international organization codes.

(U) The JOINT marking in the banner line indicates co-ownership and implied releasability of the entire document only to the co-owners. Further release requires approval of the co-owners.

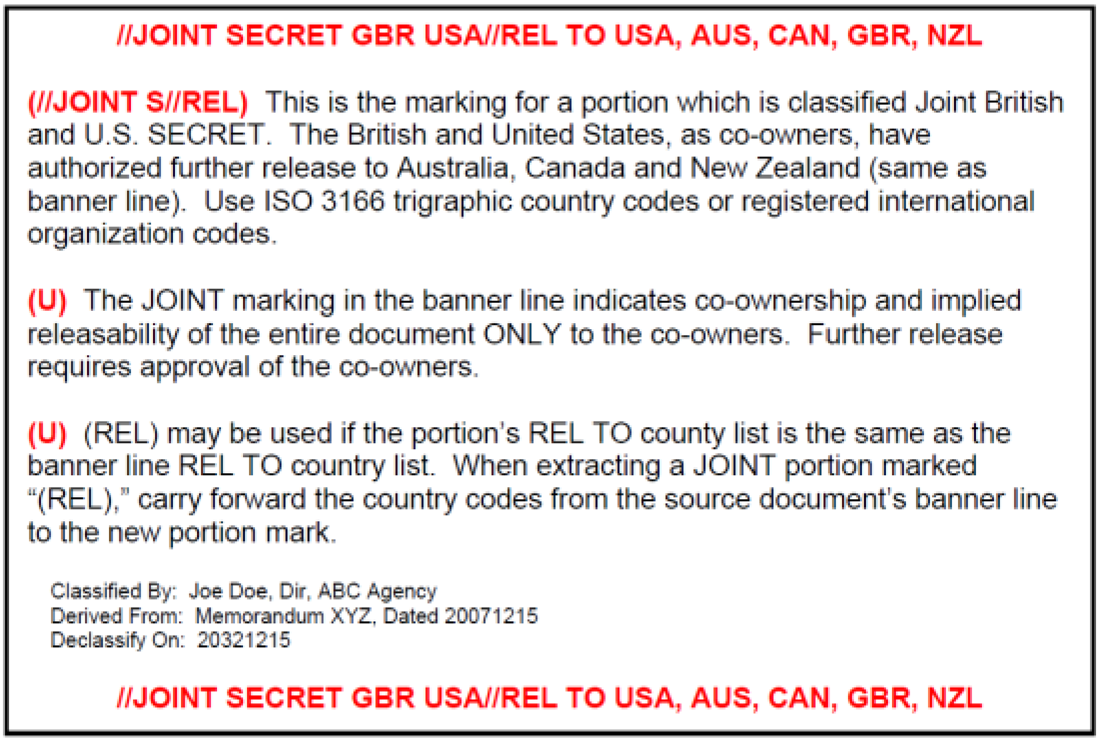
(U) The classification authority block is required on JOINT classified information when the United States is one of the co-owners.

Classified By: Joe Doe, Dir., ABC Agency
Derived From: Memorandum XYZ, Dated 20071215
Declassify On: 20321215

//JOINT SECRET CAN GBR USA

Figure 31. Example of Joint Classification Marking with REL TO

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



//JOINT SECRET GBR USA//REL TO USA, AUS, CAN, GBR, NZL

(//JOINT S//REL) This is the marking for a portion which is classified Joint British and U.S. SECRET. The British and United States, as co-owners, have authorized further release to Australia, Canada and New Zealand (same as banner line). Use ISO 3166 trigraphic country codes or registered international organization codes.

(U) The JOINT marking in the banner line indicates co-ownership and implied releasability of the entire document ONLY to the co-owners. Further release requires approval of the co-owners.

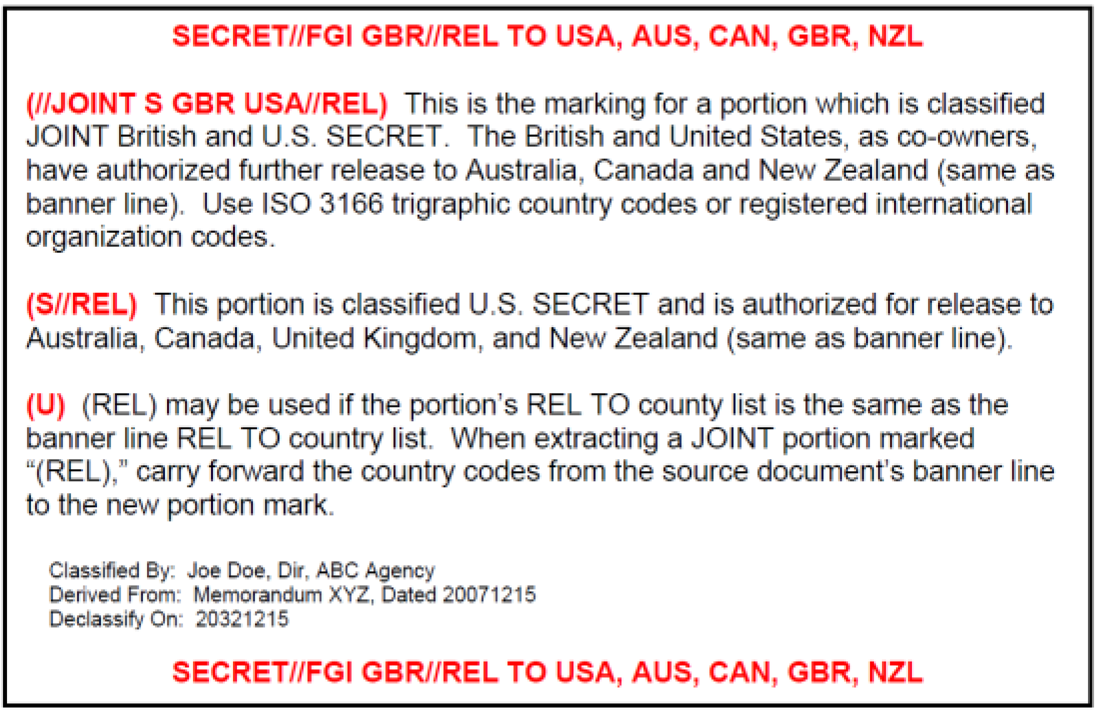
(U) (REL) may be used if the portion's REL TO county list is the same as the banner line REL TO country list. When extracting a JOINT portion marked "(REL)," carry forward the country codes from the source document's banner line to the new portion mark.

Classified By: Joe Doe, Dir, ABC Agency
Derived From: Memorandum XYZ, Dated 20071215
Declassify On: 20321215

//JOINT SECRET GBR USA//REL TO USA, AUS, CAN, GBR, NZL

Figure 32. Example of Joint Classification Marking in a U.S. Derivative Document

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



SECRET//FGI GBR//REL TO USA, AUS, CAN, GBR, NZL

(//JOINT S GBR USA//REL) This is the marking for a portion which is classified JOINT British and U.S. SECRET. The British and United States, as co-owners, have authorized further release to Australia, Canada and New Zealand (same as banner line). Use ISO 3166 trigraphic country codes or registered international organization codes.

(S//REL) This portion is classified U.S. SECRET and is authorized for release to Australia, Canada, United Kingdom, and New Zealand (same as banner line).

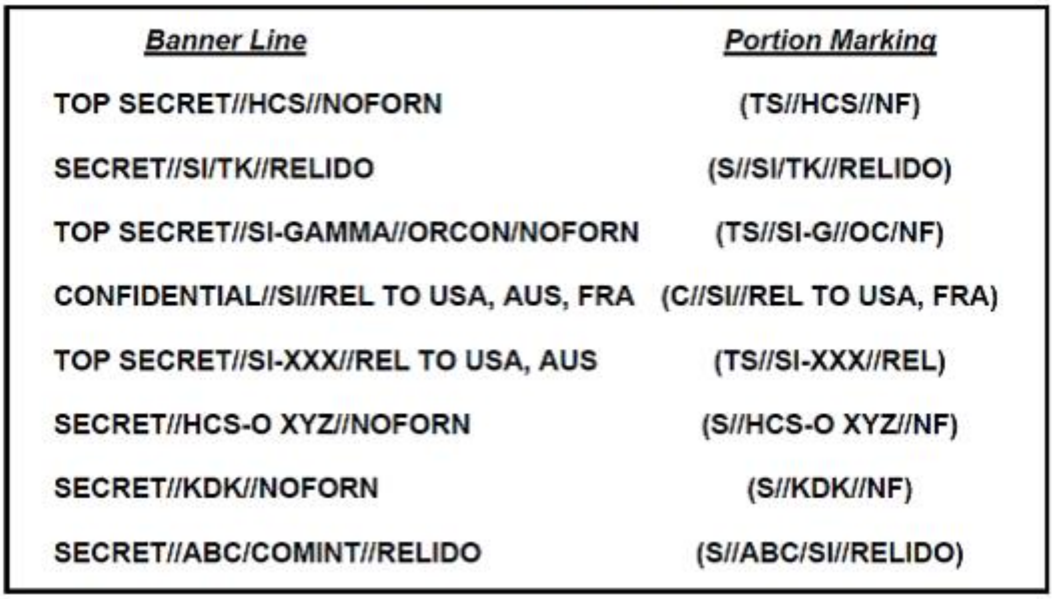
(U) (REL) may be used if the portion's REL TO county list is the same as the banner line REL TO country list. When extracting a JOINT portion marked "(REL)," carry forward the country codes from the source document's banner line to the new portion mark.

Classified By: Joe Doe, Dir, ABC Agency
Derived From: Memorandum XYZ, Dated 20071215
Declassify On: 20321215

SECRET//FGI GBR//REL TO USA, AUS, CAN, GBR, NZL

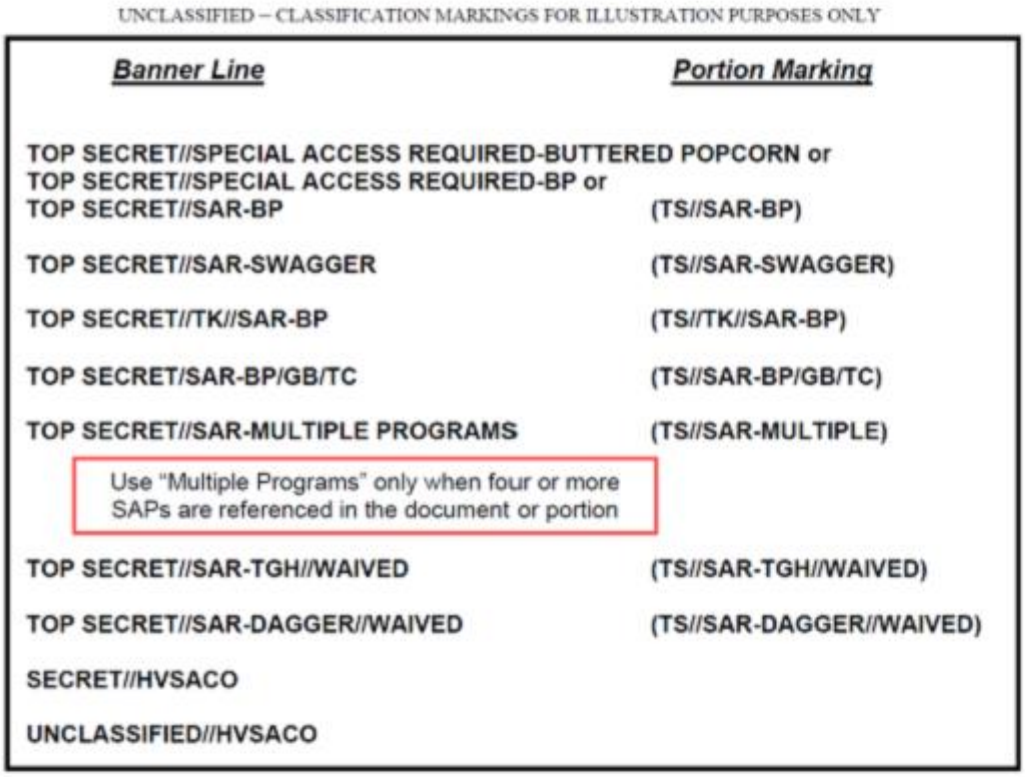
Figure 33. Examples of SCI Control Markings

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



Banner Line	***Portion Marking***
TOP SECRET//HCS//NOFORN	(TS//HCS//NF)
SECRET//SI/TK//RELIDO	(S//SI/TK//RELIDO)
TOP SECRET//SI-GAMMA//ORCON/NOFORN	(TS//SI-G//OC/NF)
CONFIDENTIAL//SI//REL TO USA, AUS, FRA	(C//SI//REL TO USA, FRA)
TOP SECRET//SI-XXX//REL TO USA, AUS	(TS//SI-XXX//REL)
SECRET//HCS-O XYZ//NOFORN	(S//HCS-O XYZ//NF)
SECRET//KDK//NOFORN	(S//KDK//NF)
SECRET//ABC/COMINT//RELIDO	(S//ABC/SI//RELIDO)

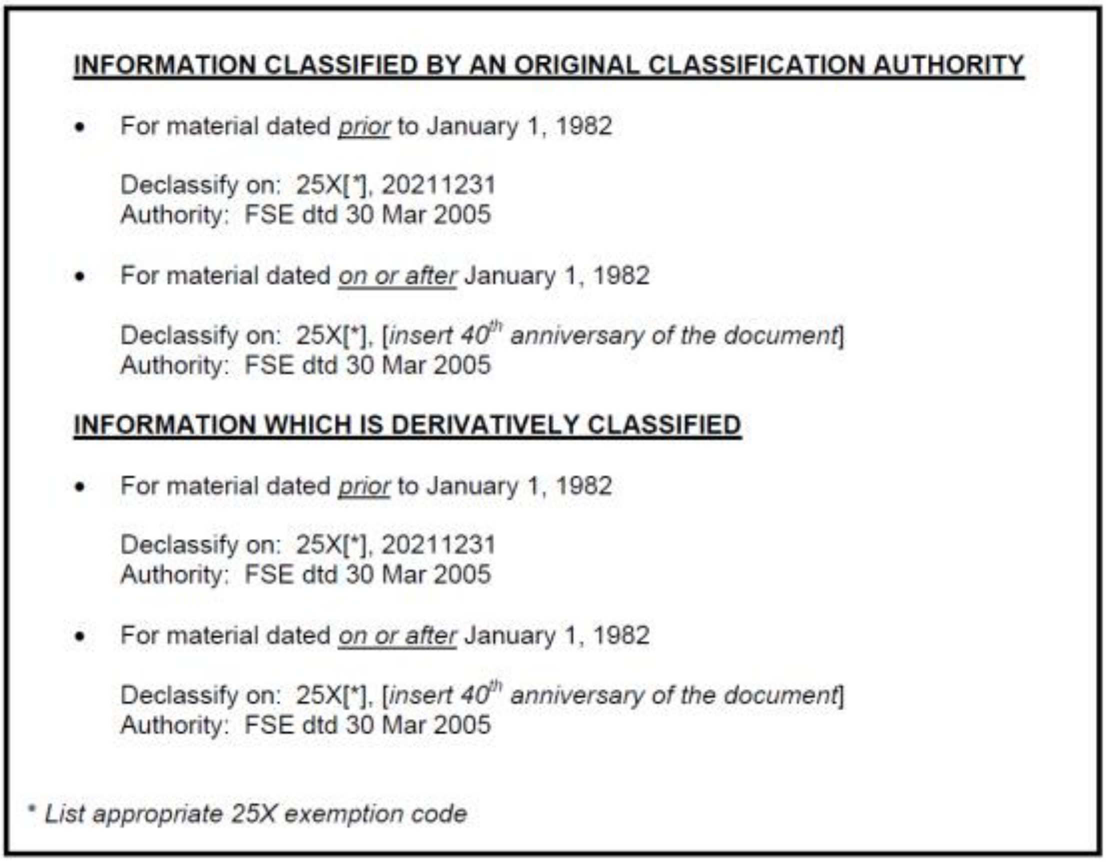
Figure 34. Examples of SAP Markings



UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

Banner Line	***Portion Marking***
TOP SECRET//SPECIAL ACCESS REQUIRED-BUTTERED POPCORN or **TOP SECRET//SPECIAL ACCESS REQUIRED-BP or** **TOP SECRET//SAR-BP**	**(TS//SAR-BP)**
TOP SECRET//SAR-SWAGGER	**(TS//SAR-SWAGGER)**
TOP SECRET//TK//SAR-BP	**(TS//TK//SAR-BP)**
TOP SECRET/SAR-BP/GB/TC	**(TS//SAR-BP/GB/TC)**
TOP SECRET//SAR-MULTIPLE PROGRAMS	**(TS//SAR-MULTIPLE)**
Use "Multiple Programs" only when four or more SAPs are referenced in the document or portion	
TOP SECRET//SAR-TGH//WAIVED	**(TS//SAR-TGH//WAIVED)**
TOP SECRET//SAR-DAGGER//WAIVED	**(TS//SAR-DAGGER//WAIVED)**
SECRET//HVSACO	
UNCLASSIFIED//HVSACO	

Figure 35. Declassification Markings for SAP Information



INFORMATION CLASSIFIED BY AN ORIGINAL CLASSIFICATION AUTHORITY

- For material dated *prior* to January 1, 1982

  Declassify on: 25X[*], 20211231
  Authority: FSE dtd 30 Mar 2005

- For material dated *on or after* January 1, 1982

  Declassify on: 25X[*], [*insert 40th anniversary of the document*]
  Authority: FSE dtd 30 Mar 2005

INFORMATION WHICH IS DERIVATIVELY CLASSIFIED

- For material dated *prior* to January 1, 1982

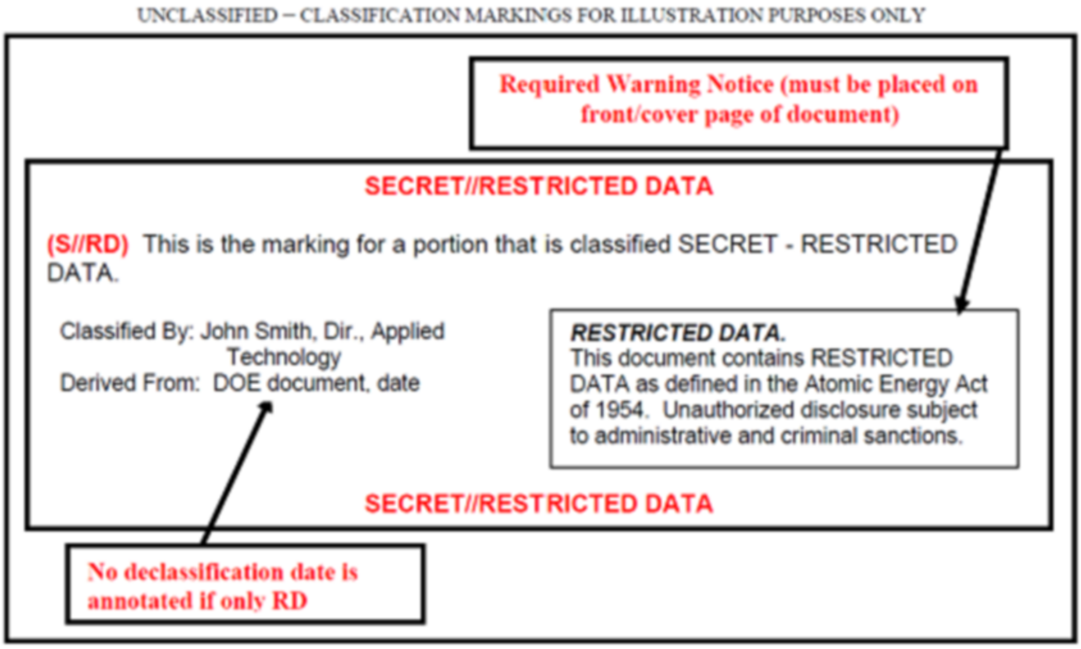
  Declassify on: 25X[*], 20211231
  Authority: FSE dtd 30 Mar 2005

- For material dated *on or after* January 1, 1982

  Declassify on: 25X[*], [*insert 40th anniversary of the document*]
  Authority: FSE dtd 30 Mar 2005

* *List appropriate 25X exemption code*

Figure 36. Example of RD Markings



UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

Required Warning Notice (must be placed on front/cover page of document)

SECRET//RESTRICTED DATA

(S//RD) This is the marking for a portion that is classified SECRET - RESTRICTED DATA.

Classified By: John Smith, Dir., Applied Technology
Derived From: DOE document, date

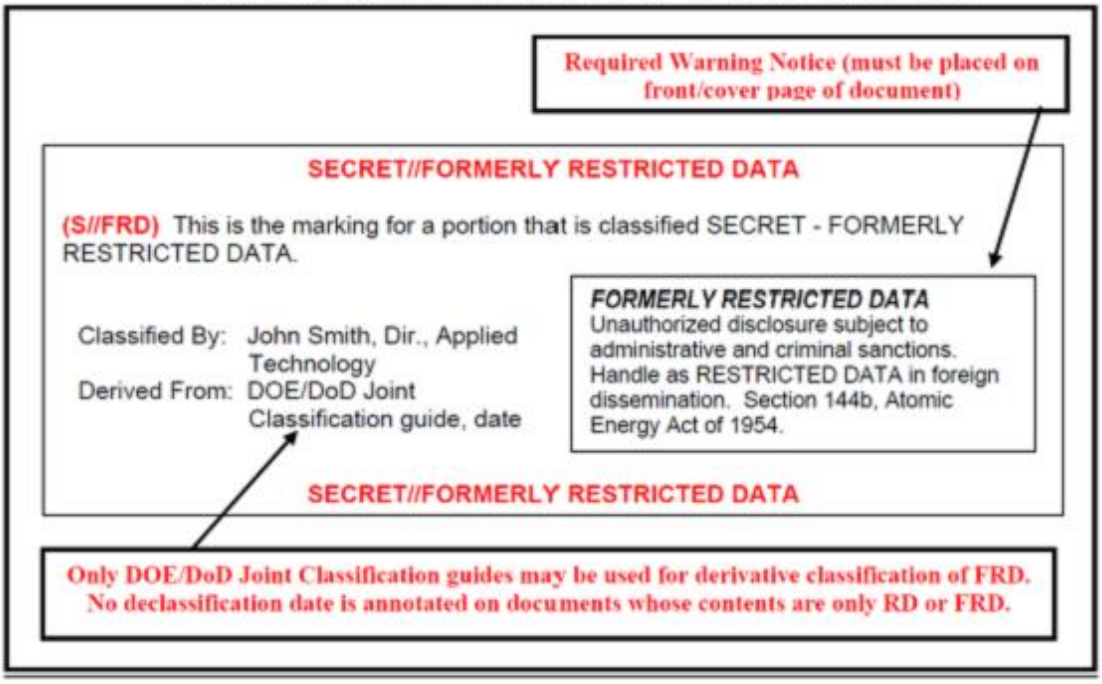
RESTRICTED DATA.
This document contains RESTRICTED DATA as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to administrative and criminal sanctions.

SECRET//RESTRICTED DATA

No declassification date is annotated if only RD

Figure 37. Example of FRD Markings

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



Required Warning Notice (must be placed on front/cover page of document)

SECRET//FORMERLY RESTRICTED DATA

(S//FRD) This is the marking for a portion that is classified SECRET - FORMERLY RESTRICTED DATA.

Classified By: John Smith, Dir., Applied Technology
Derived From: DOE/DoD Joint Classification guide, date

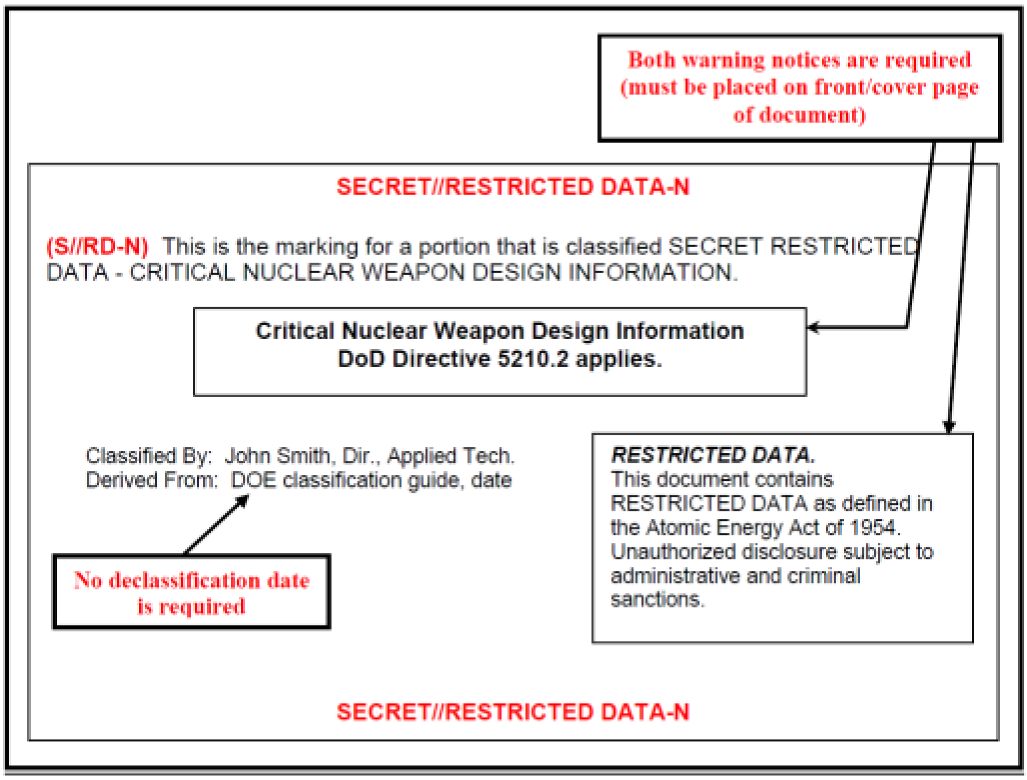
FORMERLY RESTRICTED DATA
Unauthorized disclosure subject to administrative and criminal sanctions. Handle as RESTRICTED DATA in foreign dissemination. Section 144b, Atomic Energy Act of 1954.

SECRET//FORMERLY RESTRICTED DATA

Only DOE/DoD Joint Classification guides may be used for derivative classification of FRD. No declassification date is annotated on documents whose contents are only RD or FRD.

Figure 38. Example of CNWDI Markings

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



Both warning notices are required (must be placed on front/cover page of document)

SECRET//RESTRICTED DATA-N

(S//RD-N) This is the marking for a portion that is classified SECRET RESTRICTED DATA - CRITICAL NUCLEAR WEAPON DESIGN INFORMATION.

Critical Nuclear Weapon Design Information
DoD Directive 5210.2 applies.

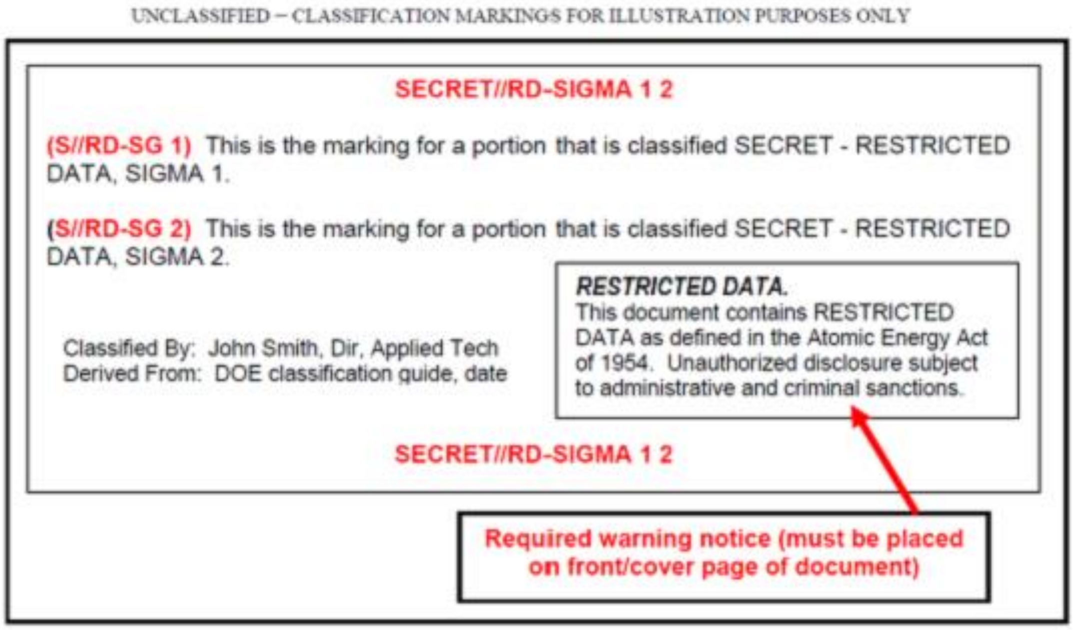
Classified By: John Smith, Dir., Applied Tech.
Derived From: DOE classification guide, date

RESTRICTED DATA.
This document contains RESTRICTED DATA as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to administrative and criminal sanctions.

No declassification date is required

SECRET//RESTRICTED DATA-N

Figure 39. Example of SIGMA Markings



UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

SECRET//RD-SIGMA 1 2

(S//RD-SG 1) This is the marking for a portion that is classified SECRET - RESTRICTED DATA, SIGMA 1.

(S//RD-SG 2) This is the marking for a portion that is classified SECRET - RESTRICTED DATA, SIGMA 2.

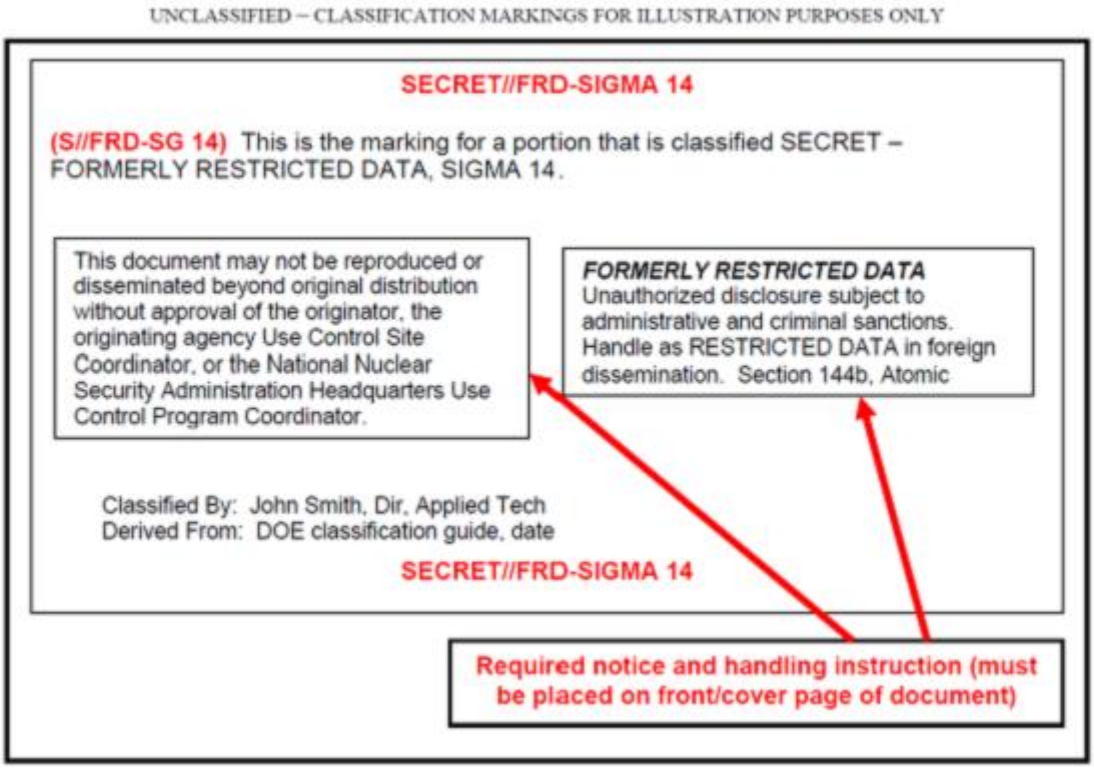
Classified By: John Smith, Dir, Applied Tech
Derived From: DOE classification guide, date

RESTRICTED DATA.
This document contains RESTRICTED DATA as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to administrative and criminal sanctions.

SECRET//RD-SIGMA 1 2

Required warning notice (must be placed on front/cover page of document)

Figure 40. Example of SIGMA 14 Markings



UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

SECRET//FRD-SIGMA 14

(S//FRD-SG 14) This is the marking for a portion that is classified SECRET – FORMERLY RESTRICTED DATA, SIGMA 14.

This document may not be reproduced or disseminated beyond original distribution without approval of the originator, the originating agency Use Control Site Coordinator, or the National Nuclear Security Administration Headquarters Use Control Program Coordinator.

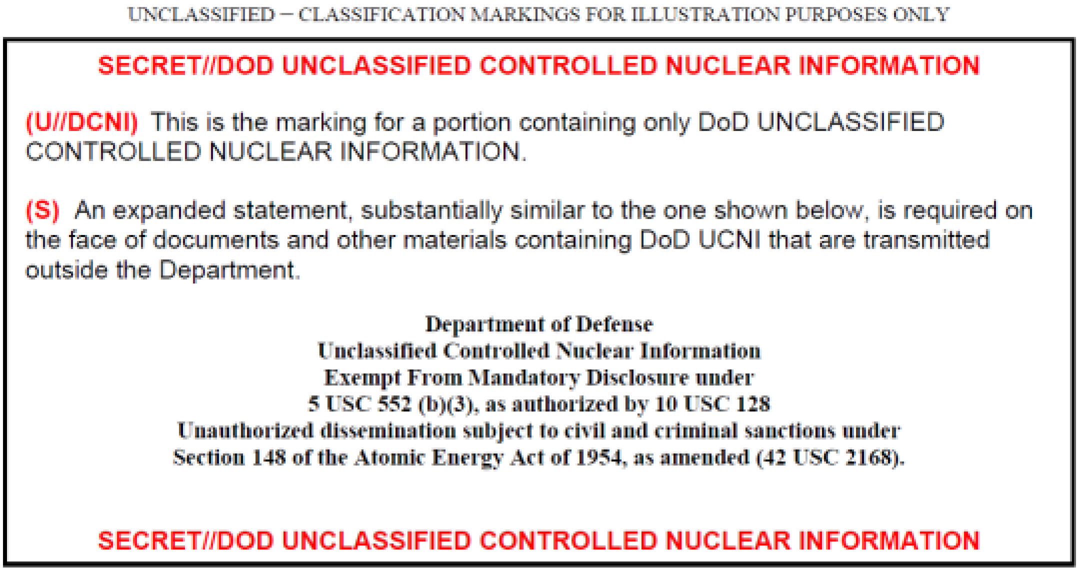
FORMERLY RESTRICTED DATA
Unauthorized disclosure subject to administrative and criminal sanctions. Handle as RESTRICTED DATA in foreign dissemination. Section 144b, Atomic

Classified By: John Smith, Dir, Applied Tech
Derived From: DOE classification guide, date

SECRET//FRD-SIGMA 14

Required notice and handling instruction (must be placed on front/cover page of document)

Figure 41. Example of DoD UCNI Marking in a Classified Document



UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

SECRET//DOD UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION

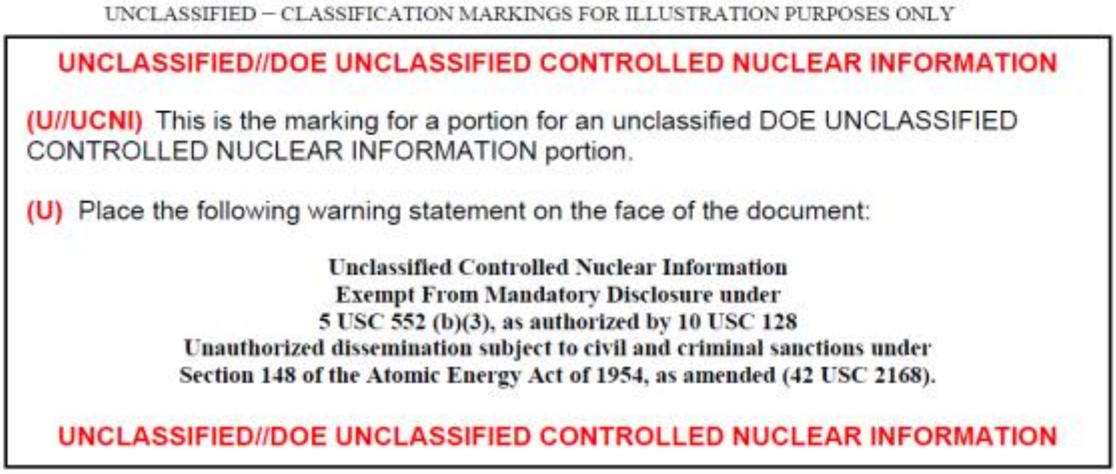
(U//DCNI) This is the marking for a portion containing only DoD UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION.

(S) An expanded statement, substantially similar to the one shown below, is required on the face of documents and other materials containing DoD UCNI that are transmitted outside the Department.

Department of Defense
Unclassified Controlled Nuclear Information
Exempt From Mandatory Disclosure under
5 USC 552 (b)(3), as authorized by 10 USC 128
Unauthorized dissemination subject to civil and criminal sanctions under
Section 148 of the Atomic Energy Act of 1954, as amended (42 USC 2168).

SECRET//DOD UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION

Figure 42. Example of DOE UCNI Marking



UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

UNCLASSIFIED//DOE UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION

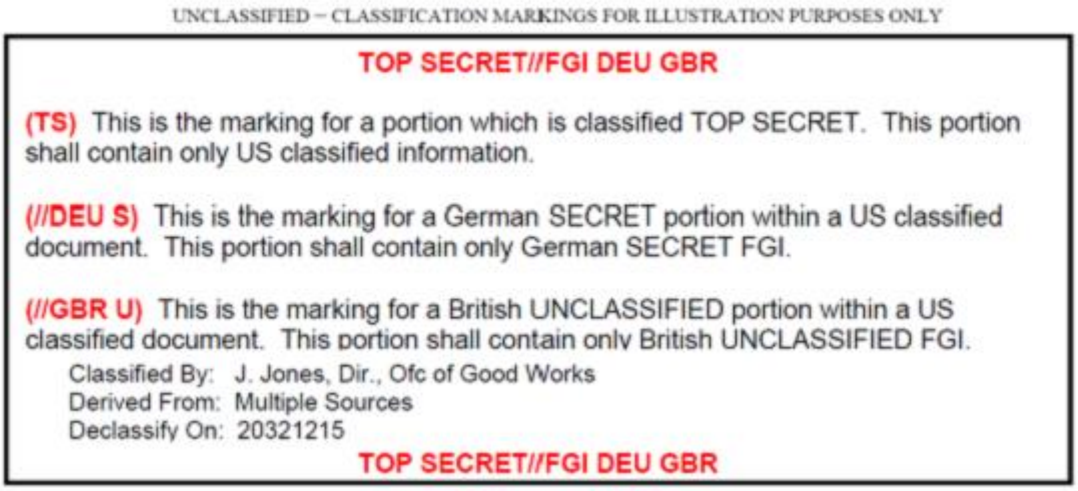
(U//UCNI) This is the marking for a portion for an unclassified DOE UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION portion.

(U) Place the following warning statement on the face of the document:

Unclassified Controlled Nuclear Information
Exempt From Mandatory Disclosure under
5 USC 552 (b)(3), as authorized by 10 USC 128
Unauthorized dissemination subject to civil and criminal sanctions under
Section 148 of the Atomic Energy Act of 1954, as amended (42 USC 2168).

UNCLASSIFIED//DOE UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION

Figure 43. Example of FGI Marking



UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

TOP SECRET//FGI DEU GBR

(TS) This is the marking for a portion which is classified TOP SECRET. This portion shall contain only US classified information.

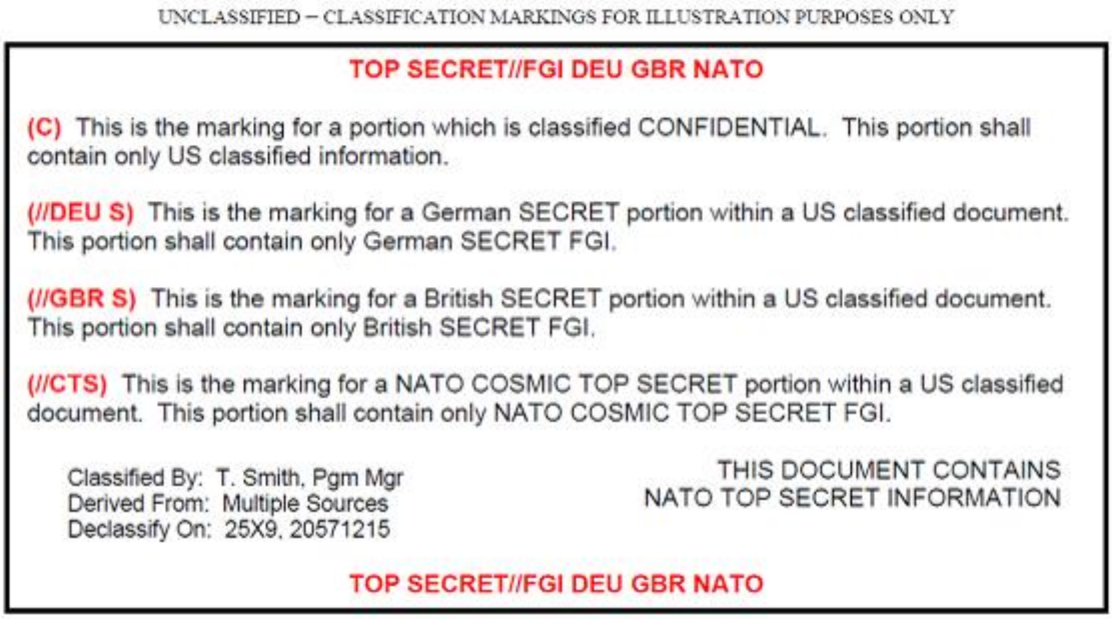
(//DEU S) This is the marking for a German SECRET portion within a US classified document. This portion shall contain only German SECRET FGI.

(//GBR U) This is the marking for a British UNCLASSIFIED portion within a US classified document. This portion shall contain only British UNCLASSIFIED FGI.

Classified By: J. Jones, Dir., Ofc of Good Works
Derived From: Multiple Sources
Declassify On: 20321215

TOP SECRET//FGI DEU GBR

Figure 44. Example of FGI Marking with NATO Information



UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

TOP SECRET//FGI DEU GBR NATO

(C) This is the marking for a portion which is classified CONFIDENTIAL. This portion shall contain only US classified information.

(//DEU S) This is the marking for a German SECRET portion within a US classified document. This portion shall contain only German SECRET FGI.

(//GBR S) This is the marking for a British SECRET portion within a US classified document. This portion shall contain only British SECRET FGI.

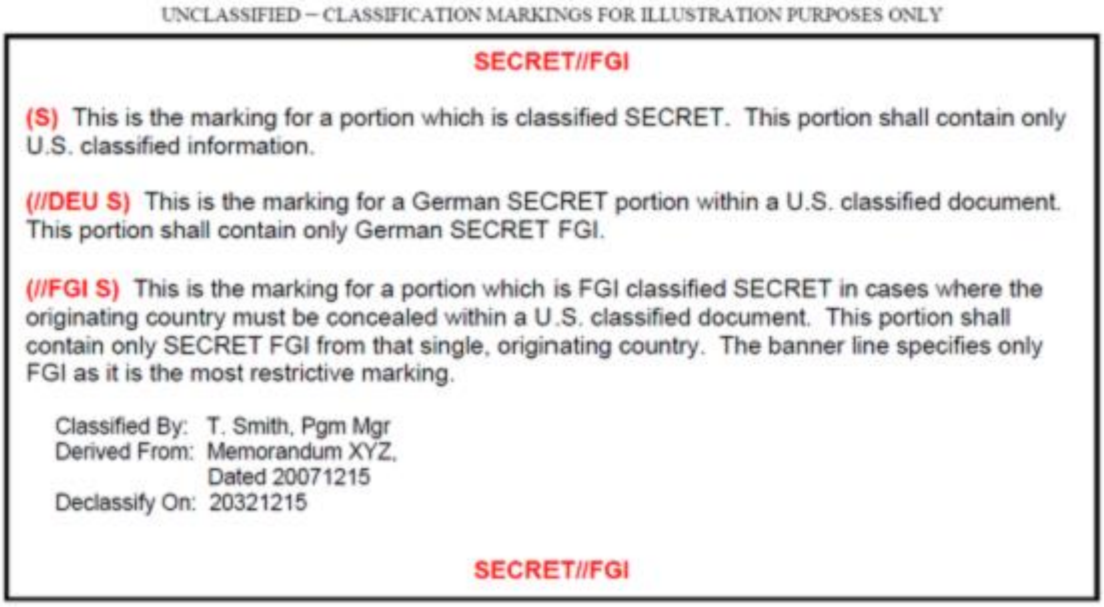
(//CTS) This is the marking for a NATO COSMIC TOP SECRET portion within a US classified document. This portion shall contain only NATO COSMIC TOP SECRET FGI.

Classified By: T. Smith, Pgm Mgr
Derived From: Multiple Sources
Declassify On: 25X9, 20571215

THIS DOCUMENT CONTAINS
NATO TOP SECRET INFORMATION

TOP SECRET//FGI DEU GBR NATO

Figure 45. Example of FGI Marking When Originating Country Is Concealed



UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

SECRET//FGI

(S) This is the marking for a portion which is classified SECRET. This portion shall contain only U.S. classified information.

(//DEU S) This is the marking for a German SECRET portion within a U.S. classified document. This portion shall contain only German SECRET FGI.

(//FGI S) This is the marking for a portion which is FGI classified SECRET in cases where the originating country must be concealed within a U.S. classified document. This portion shall contain only SECRET FGI from that single, originating country. The banner line specifies only FGI as it is the most restrictive marking.

Classified By: T. Smith, Pgm Mgr
Derived From: Memorandum XYZ,
Dated 20071215
Declassify On: 20321215

SECRET//FGI

Figure 46. Example of FGI Marking with REL TO

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

TOP SECRET//FGI CAN DEU

(S//REL TO USA, AUS) This is the marking for a portion that is releasable to Australia within a U.S. classified document. This portion shall contain only U.S. classified information that is releasable to Australia.

(//CAN S//REL TO USA, AUS, CAN, GBR) This is the marking for a Canadian SECRET portion for which Canada has allowed release back to Canada and further release to Australia and Great Britain within a U.S. classified document. This portion shall contain only Canadian SECRET FGI releasable to those countries listed.

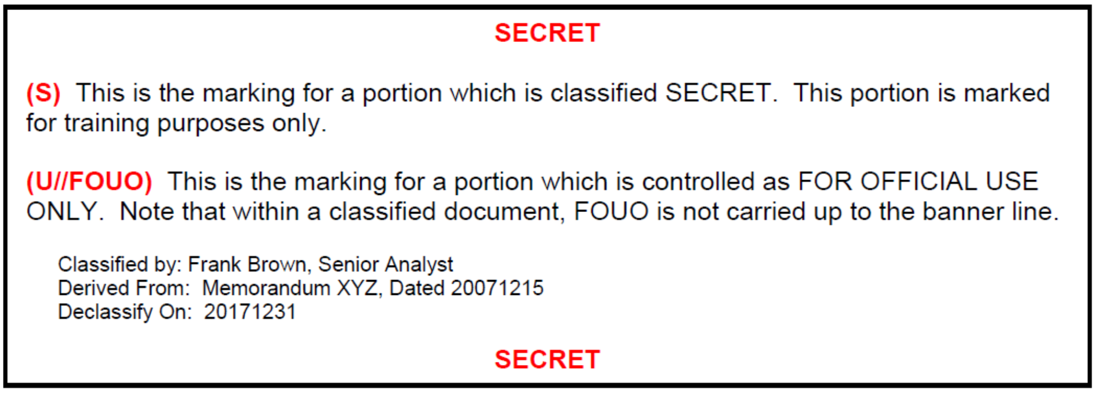
(//DEU TS) This is the marking for a German TOP SECRET portion within a U.S. classified document. This portion shall contain only German TOP SECRET FGI.

Classified By: T. Smith, Pgm Mgr
Derived From: Memorandum XYZ,
Dated 20071215
Declassify On: 20321215

TOP SECRET//FGI CAN DEU

Figure 47. Example of FOUO Marking in a Classified Document

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



SECRET

(S) This is the marking for a portion which is classified SECRET. This portion is marked for training purposes only.

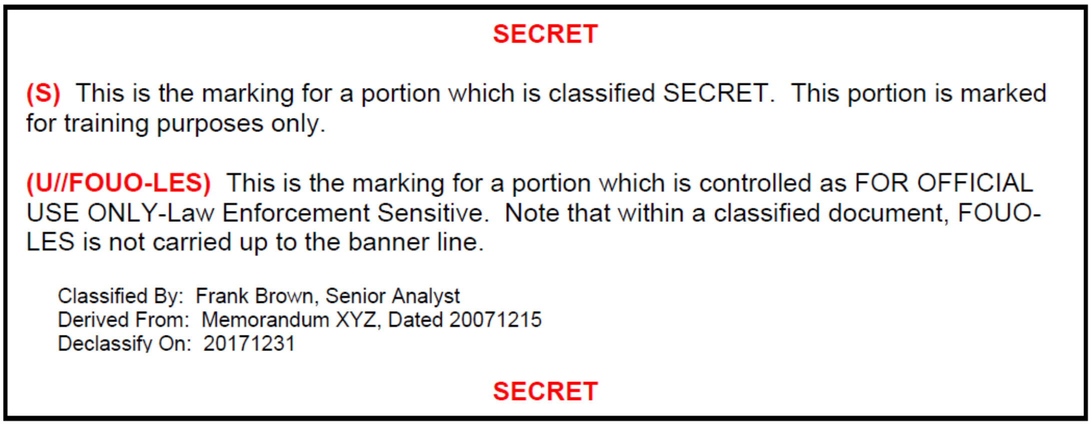
(U//FOUO) This is the marking for a portion which is controlled as FOR OFFICIAL USE ONLY. Note that within a classified document, FOUO is not carried up to the banner line.

Classified by: Frank Brown, Senior Analyst
Derived From: Memorandum XYZ, Dated 20071215
Declassify On: 20171231

SECRET

Figure 48. Example of FOUO-LES Marking in a Classified Document

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



SECRET

(S) This is the marking for a portion which is classified SECRET. This portion is marked for training purposes only.

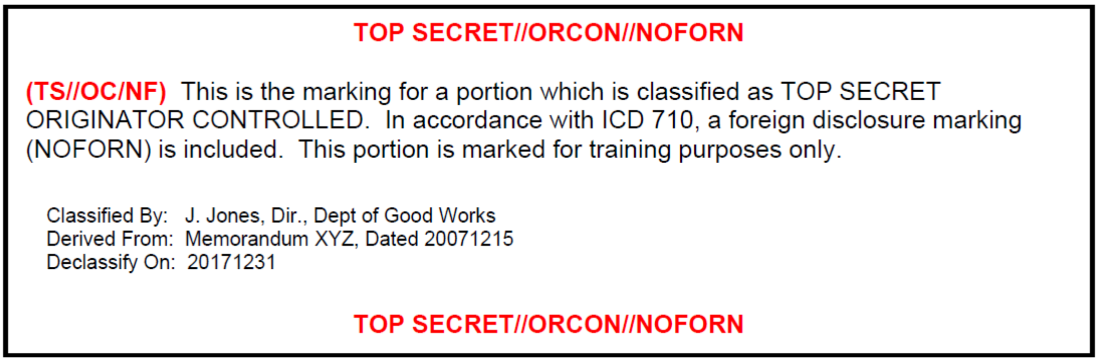
(U//FOUO-LES) This is the marking for a portion which is controlled as FOR OFFICIAL USE ONLY-Law Enforcement Sensitive. Note that within a classified document, FOUO-LES is not carried up to the banner line.

Classified By: Frank Brown, Senior Analyst
Derived From: Memorandum XYZ, Dated 20071215
Declassify On: 20171231

SECRET

Figure 49. Example of ORCON Marking

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



TOP SECRET//ORCON//NOFORN

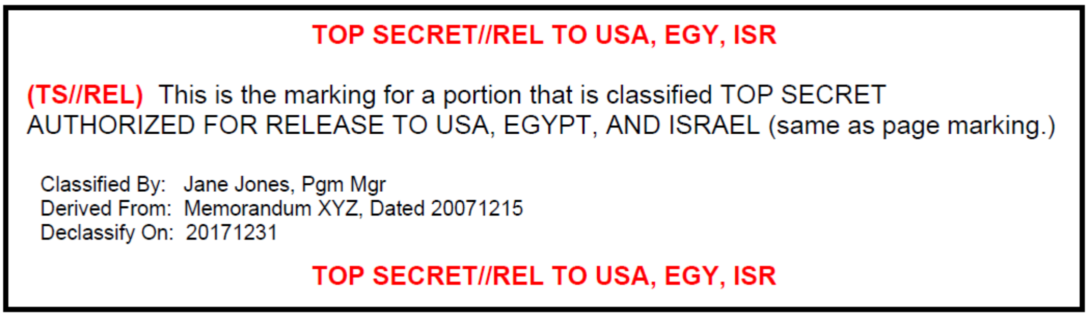
(TS//OC/NF) This is the marking for a portion which is classified as TOP SECRET ORIGINATOR CONTROLLED. In accordance with ICD 710, a foreign disclosure marking (NOFORN) is included. This portion is marked for training purposes only.

Classified By: J. Jones, Dir., Dept of Good Works
Derived From: Memorandum XYZ, Dated 20071215
Declassify On: 20171231

TOP SECRET//ORCON//NOFORN

Figure 50. Example of REL TO Marking

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



TOP SECRET//REL TO USA, EGY, ISR

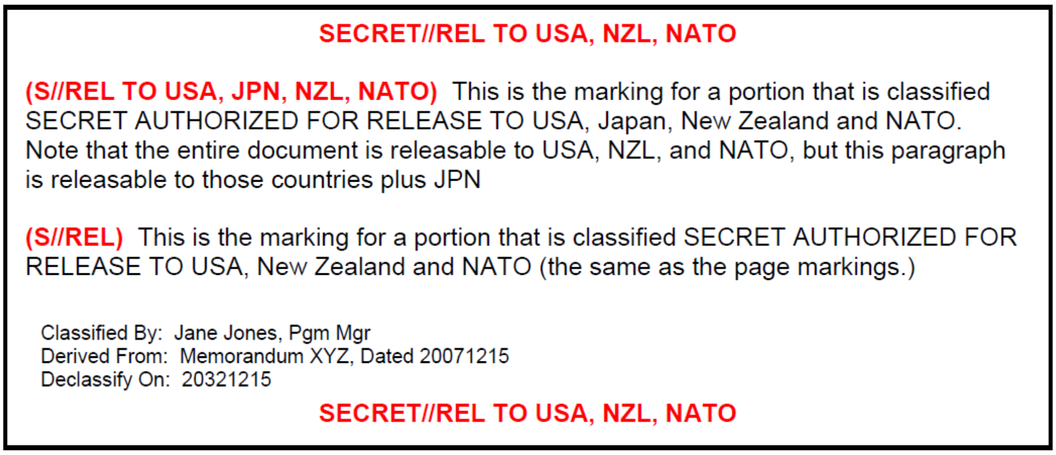
(TS//REL) This is the marking for a portion that is classified TOP SECRET AUTHORIZED FOR RELEASE TO USA, EGYPT, AND ISRAEL (same as page marking.)

Classified By: Jane Jones, Pgm Mgr
Derived From: Memorandum XYZ, Dated 20071215
Declassify On: 20171231

TOP SECRET//REL TO USA, EGY, ISR

Figure 51. Example of REL TO Marking When Not All Portions Are Equally Releasable

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



SECRET//REL TO USA, NZL, NATO

(S//REL TO USA, JPN, NZL, NATO) This is the marking for a portion that is classified SECRET AUTHORIZED FOR RELEASE TO USA, Japan, New Zealand and NATO. Note that the entire document is releasable to USA, NZL, and NATO, but this paragraph is releasable to those countries plus JPN

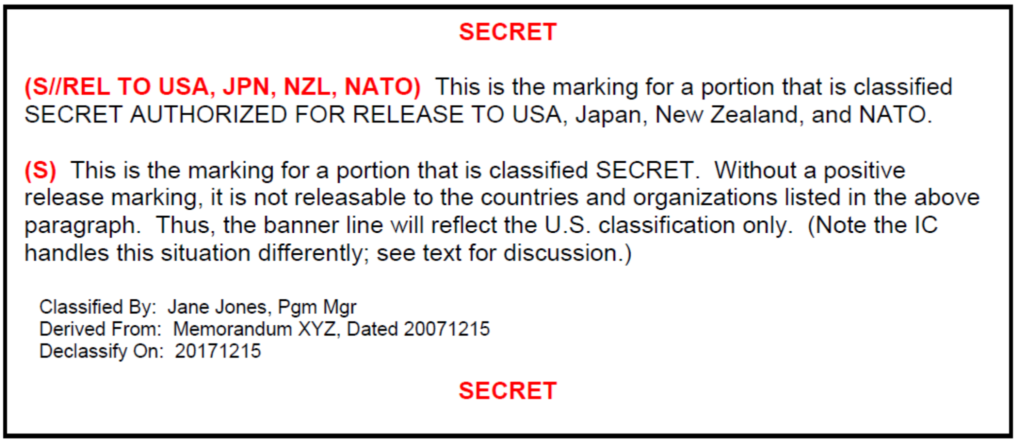
(S//REL) This is the marking for a portion that is classified SECRET AUTHORIZED FOR RELEASE TO USA, New Zealand and NATO (the same as the page markings.)

Classified By: Jane Jones, Pgm Mgr
Derived From: Memorandum XYZ, Dated 20071215
Declassify On: 20321215

SECRET//REL TO USA, NZL, NATO

Figure 52. Example of REL TO Marking When Portions Lack Explicit Release Markings

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



SECRET

(S//REL TO USA, JPN, NZL, NATO) This is the marking for a portion that is classified SECRET AUTHORIZED FOR RELEASE TO USA, Japan, New Zealand, and NATO.

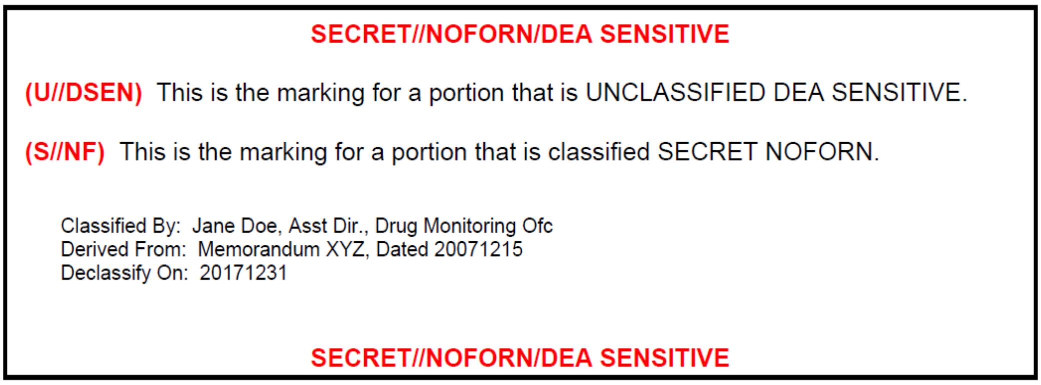
(S) This is the marking for a portion that is classified SECRET. Without a positive release marking, it is not releasable to the countries and organizations listed in the above paragraph. Thus, the banner line will reflect the U.S. classification only. (Note the IC handles this situation differently; see text for discussion.)

Classified By: Jane Jones, Pgm Mgr
Derived From: Memorandum XYZ, Dated 20071215
Declassify On: 20171215

SECRET

Figure 53. Example of DEA SENSITIVE Marking in a Classified Document

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



SECRET//NOFORN/DEA SENSITIVE

(U//DSEN) This is the marking for a portion that is UNCLASSIFIED DEA SENSITIVE.

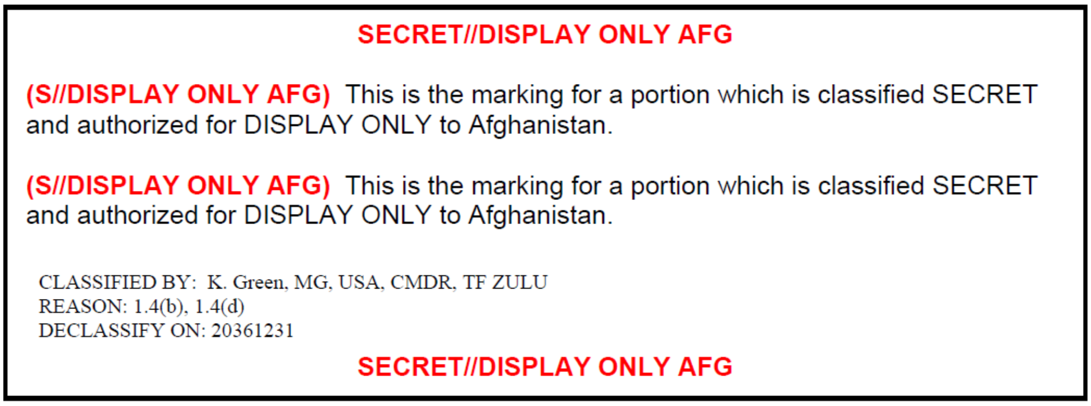
(S//NF) This is the marking for a portion that is classified SECRET NOFORN.

Classified By: Jane Doe, Asst Dir., Drug Monitoring Ofc
Derived From: Memorandum XYZ, Dated 20071215
Declassify On: 20171231

SECRET//NOFORN/DEA SENSITIVE

Figure 54. Example of DISPLAY ONLY Marking

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



SECRET//DISPLAY ONLY AFG

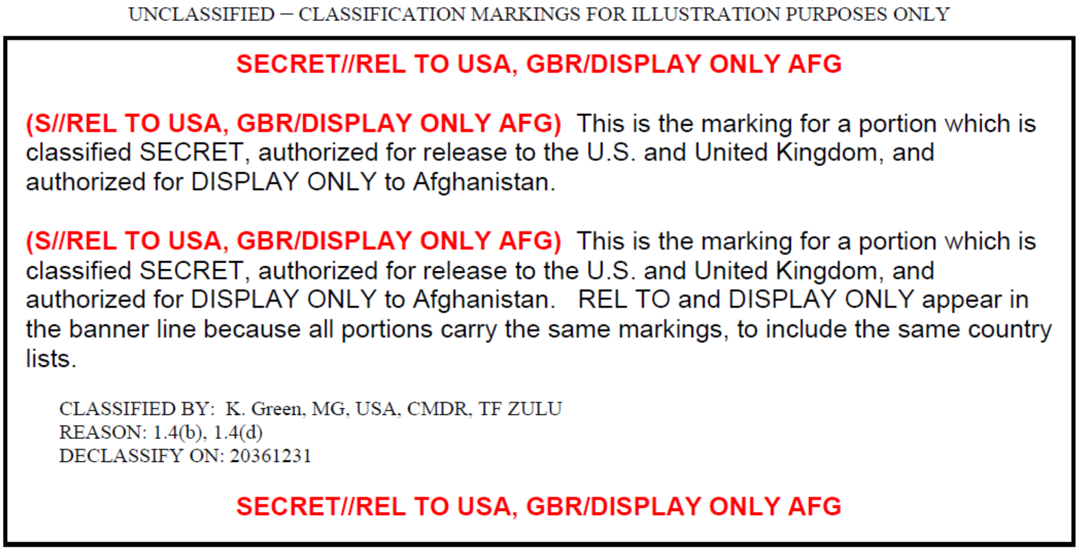
(S//DISPLAY ONLY AFG) This is the marking for a portion which is classified SECRET and authorized for DISPLAY ONLY to Afghanistan.

(S//DISPLAY ONLY AFG) This is the marking for a portion which is classified SECRET and authorized for DISPLAY ONLY to Afghanistan.

CLASSIFIED BY: K. Green, MG, USA, CMDR, TF ZULU
REASON: 1.4(b), 1.4(d)
DECLASSIFY ON: 20361231

SECRET//DISPLAY ONLY AFG

Figure 55. Example of DISPLAY ONLY Marking with REL TO



UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

SECRET//REL TO USA, GBR/DISPLAY ONLY AFG

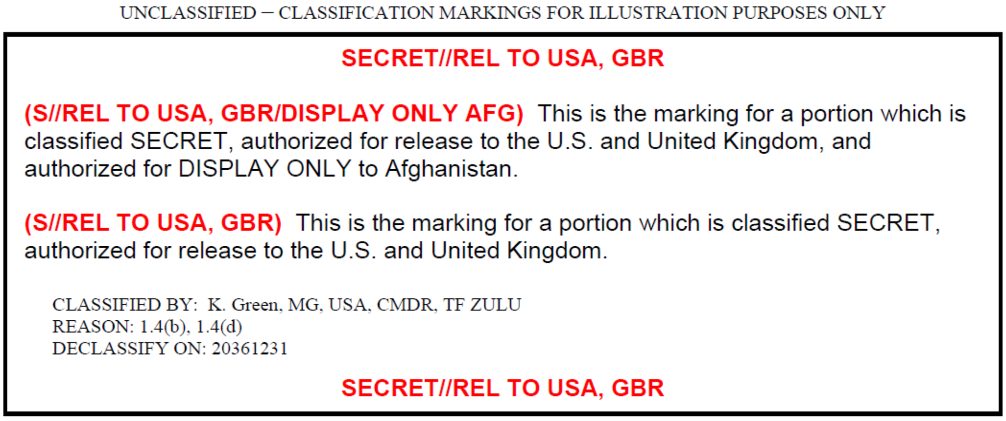
(S//REL TO USA, GBR/DISPLAY ONLY AFG) This is the marking for a portion which is classified SECRET, authorized for release to the U.S. and United Kingdom, and authorized for DISPLAY ONLY to Afghanistan.

(S//REL TO USA, GBR/DISPLAY ONLY AFG) This is the marking for a portion which is classified SECRET, authorized for release to the U.S. and United Kingdom, and authorized for DISPLAY ONLY to Afghanistan. REL TO and DISPLAY ONLY appear in the banner line because all portions carry the same markings, to include the same country lists.

CLASSIFIED BY: K. Green, MG, USA, CMDR, TF ZULU
REASON: 1.4(b), 1.4(d)
DECLASSIFY ON: 20361231

SECRET//REL TO USA, GBR/DISPLAY ONLY AFG

Figure 56. Example of DISPLAY ONLY Marking When Not All Portions are DISPLAY ONLY



UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

SECRET//REL TO USA, GBR

(S//REL TO USA, GBR/DISPLAY ONLY AFG) This is the marking for a portion which is classified SECRET, authorized for release to the U.S. and United Kingdom, and authorized for DISPLAY ONLY to Afghanistan.

(S//REL TO USA, GBR) This is the marking for a portion which is classified SECRET, authorized for release to the U.S. and United Kingdom.

CLASSIFIED BY: K. Green, MG, USA, CMDR, TF ZULU
REASON: 1.4(b), 1.4(d)
DECLASSIFY ON: 20361231

SECRET//REL TO USA, GBR

Figure 57. Example of DISPLAY ONLY Marking In Mixed Releasability Situation

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

SECRET

(S//REL TO USA, IRQ) This is the marking for a portion which is classified SECRET authorized for release to the U.S. and Iraq.

(S//DISPLAY ONLY AFG) This is the marking for a portion which is classified SECRET and authorized for DISPLAY ONLY to Afghanistan.

(S) This is a portion which is classified SECRET. Further release and/or disclosure must be determined by a foreign disclosure officer.

CLASSIFIED BY: K. Green, MG, USA, CMDR, TF ZULU
REASON: 1.4(b), 1.4(d)
DECLASSIFY ON: 20361231

SECRET

Figure 58. Example of LIMDIS Marking

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

UNCLASSIFIED//LIMITED DISTRIBUTION

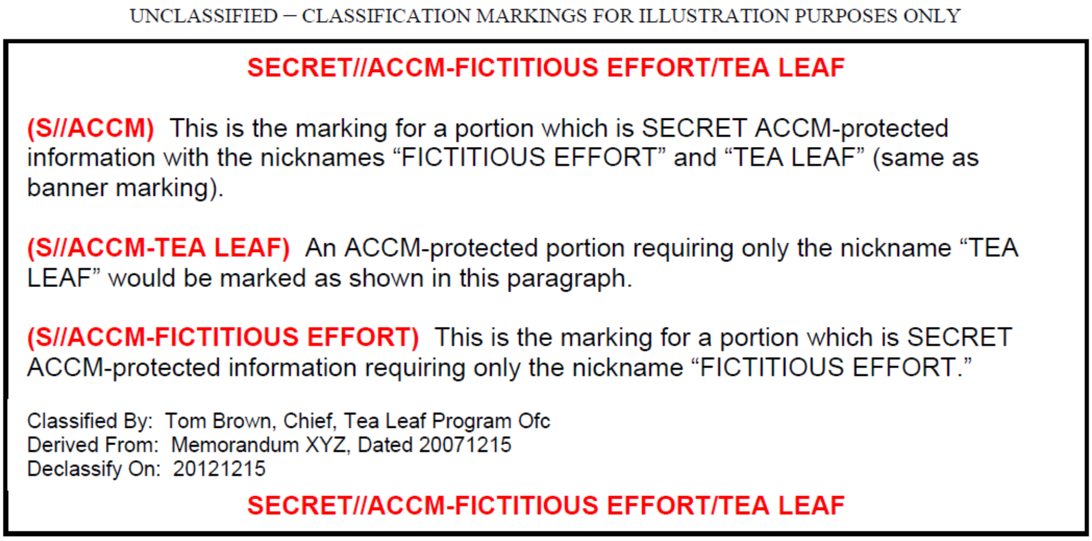
(U//DS) This is the marking for a portion that is UNCLASSIFIED LIMITED DISTRIBUTION. This portion is marked for training purposes only.

(U) The notice below is required on the front of each document containing LIMDIS:

Distribution authorized to DoD, IAW 10 U.S.C.130 & 455. Release authorized to U.S. DoD contractors IAW 48 C.F.R. 252.245-7000. Refer other requests to: Headquarters, NGA, ATTN: Release Officer, Mail Stop S82-OIAD, 7500 Geoint Drive, Springfield, VA 22150-7500. Destroy IAW DoDM 5200.01. **Removal of this caveat is prohibited.**

UNCLASSIFIED//LIMITED DISTRIBUTION

Figure 59. Example of ACCM Markings



UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

SECRET//ACCM-FICTITIOUS EFFORT/TEA LEAF

(S//ACCM) This is the marking for a portion which is SECRET ACCM-protected information with the nicknames “FICTITIOUS EFFORT” and “TEA LEAF” (same as banner marking).

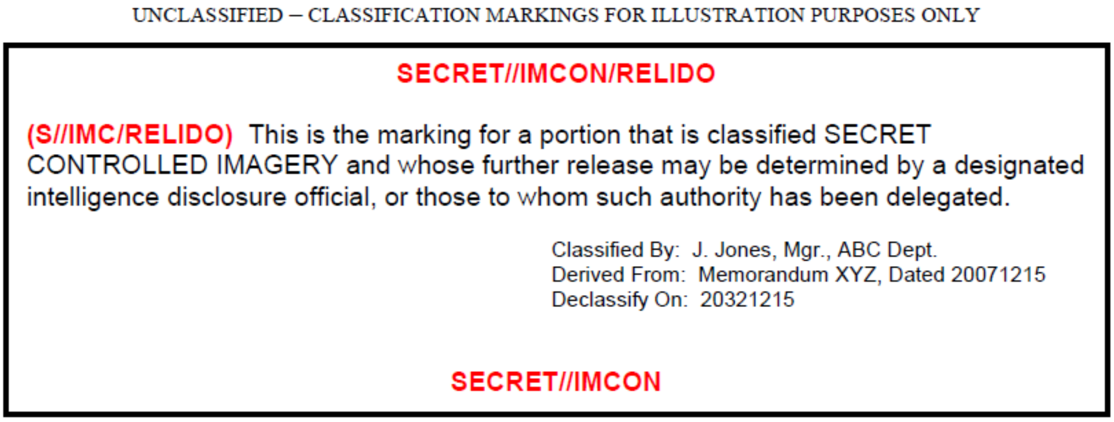
(S//ACCM-TEA LEAF) An ACCM-protected portion requiring only the nickname “TEA LEAF” would be marked as shown in this paragraph.

(S//ACCM-FICTITIOUS EFFORT) This is the marking for a portion which is SECRET ACCM-protected information requiring only the nickname “FICTITIOUS EFFORT.”

Classified By: Tom Brown, Chief, Tea Leaf Program Ofc
Derived From: Memorandum XYZ, Dated 20071215
Declassify On: 20121215

SECRET//ACCM-FICTITIOUS EFFORT/TEA LEAF

Figure 60. Example of IMCON Marking



UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

SECRET//IMCON/RELIDO

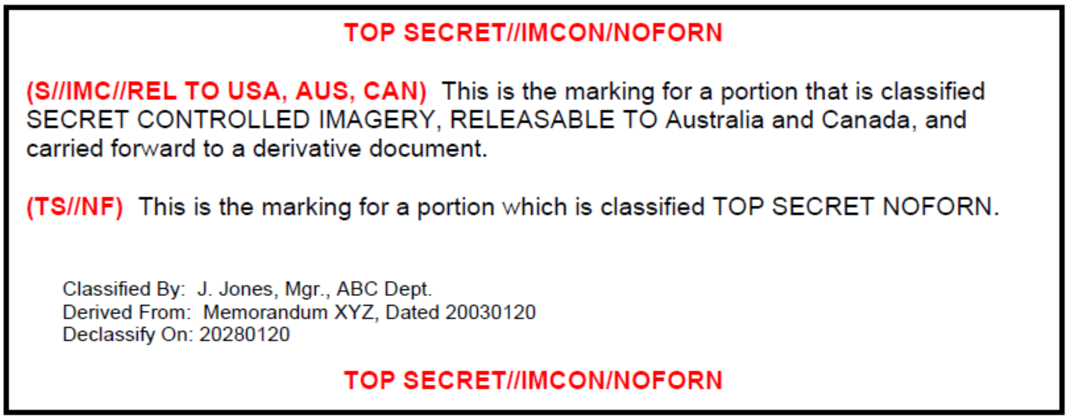
(S//IMC/RELIDO) This is the marking for a portion that is classified SECRET CONTROLLED IMAGERY and whose further release may be determined by a designated intelligence disclosure official, or those to whom such authority has been delegated.

Classified By: J. Jones, Mgr., ABC Dept.
Derived From: Memorandum XYZ, Dated 20071215
Declassify On: 20321215

SECRET//IMCON

Figure 61. Example of IMCON Banner Marking When There Are NOFORN Portions

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



TOP SECRET//IMCON/NOFORN

(S//IMC//REL TO USA, AUS, CAN) This is the marking for a portion that is classified SECRET CONTROLLED IMAGERY, RELEASABLE TO Australia and Canada, and carried forward to a derivative document.

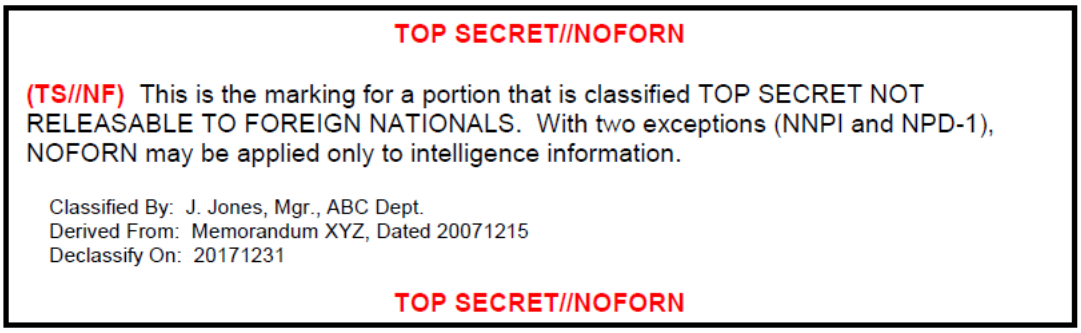
(TS//NF) This is the marking for a portion which is classified TOP SECRET NOFORN.

Classified By: J. Jones, Mgr., ABC Dept.
Derived From: Memorandum XYZ, Dated 20030120
Declassify On: 20280120

TOP SECRET//IMCON/NOFORN

Figure 62. Example of NOFORN Marking

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



TOP SECRET//NOFORN

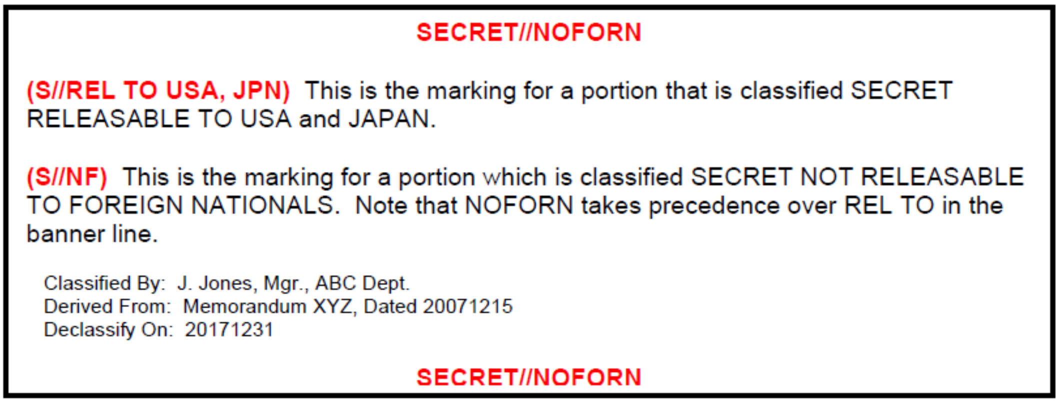
(TS//NF) This is the marking for a portion that is classified TOP SECRET NOT RELEASABLE TO FOREIGN NATIONALS. With two exceptions (NNPI and NPD-1), NOFORN may be applied only to intelligence information.

Classified By: J. Jones, Mgr., ABC Dept.
Derived From: Memorandum XYZ, Dated 20071215
Declassify On: 20171231

TOP SECRET//NOFORN

Figure 63. Example of NOFORN Markings with REL TO Portions

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



SECRET//NOFORN

(S//REL TO USA, JPN) This is the marking for a portion that is classified SECRET RELEASABLE TO USA and JAPAN.

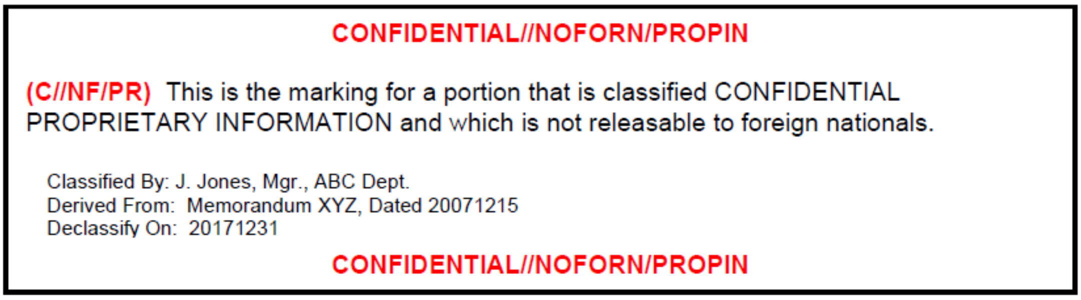
(S//NF) This is the marking for a portion which is classified SECRET NOT RELEASABLE TO FOREIGN NATIONALS. Note that NOFORN takes precedence over REL TO in the banner line.

Classified By: J. Jones, Mgr., ABC Dept.
Derived From: Memorandum XYZ, Dated 20071215
Declassify On: 20171231

SECRET//NOFORN

Figure 64. Example of PROPIN Marking

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



CONFIDENTIAL//NOFORN/PROPIN

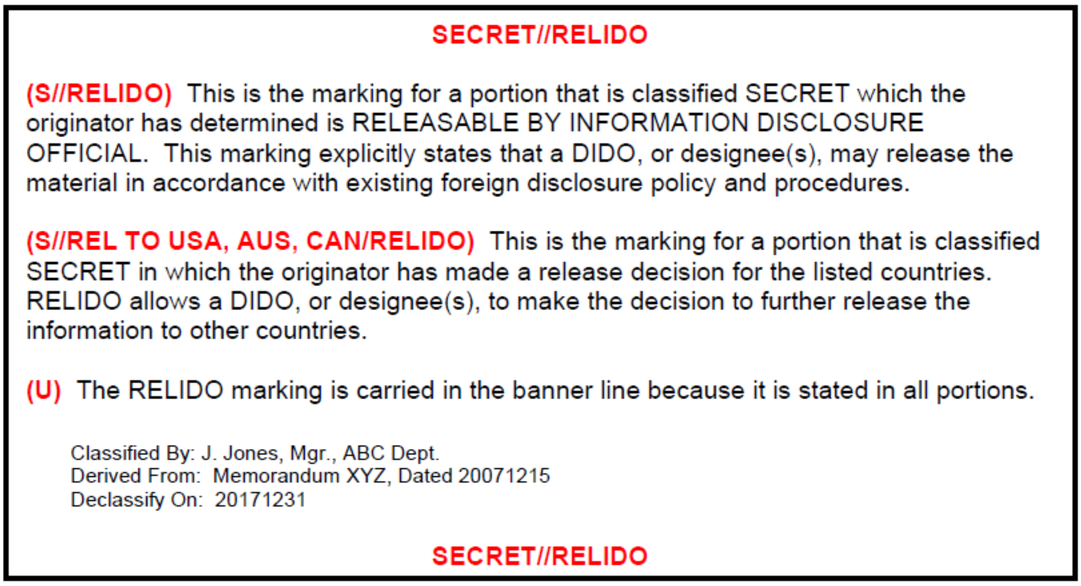
(C//NF/PR) This is the marking for a portion that is classified CONFIDENTIAL PROPRIETARY INFORMATION and which is not releasable to foreign nationals.

Classified By: J. Jones, Mgr., ABC Dept.
Derived From: Memorandum XYZ, Dated 20071215
Declassify On: 20171231

CONFIDENTIAL//NOFORN/PROPIN

Figure 65. Example of RELIDO Marking

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



SECRET//RELIDO

(S//RELIDO) This is the marking for a portion that is classified SECRET which the originator has determined is RELEASABLE BY INFORMATION DISCLOSURE OFFICIAL. This marking explicitly states that a DIDO, or designee(s), may release the material in accordance with existing foreign disclosure policy and procedures.

(S//REL TO USA, AUS, CAN/RELIDO) This is the marking for a portion that is classified SECRET in which the originator has made a release decision for the listed countries. RELIDO allows a DIDO, or designee(s), to make the decision to further release the information to other countries.

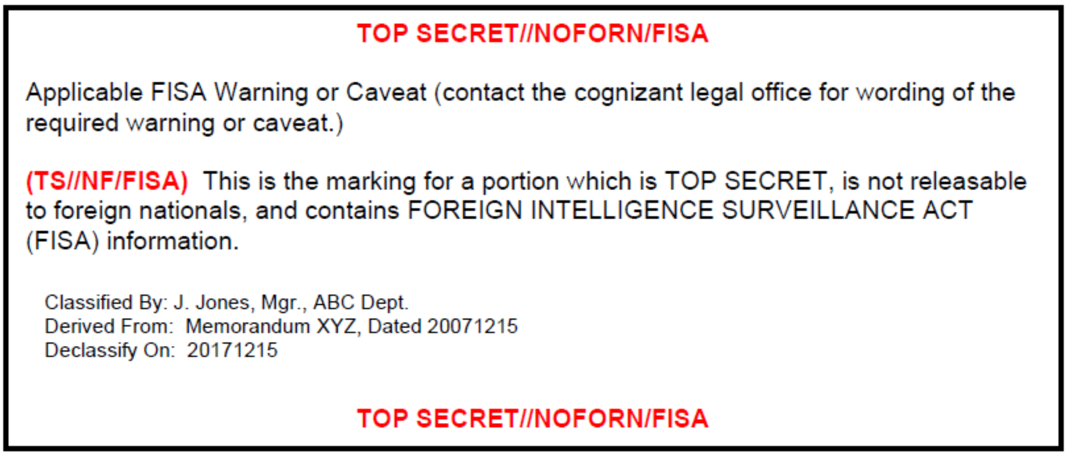
(U) The RELIDO marking is carried in the banner line because it is stated in all portions.

Classified By: J. Jones, Mgr., ABC Dept.
Derived From: Memorandum XYZ, Dated 20071215
Declassify On: 20171231

SECRET//RELIDO

Figure 66. Example of FISA Marking

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



TOP SECRET//NOFORN/FISA

Applicable FISA Warning or Caveat (contact the cognizant legal office for wording of the required warning or caveat.)

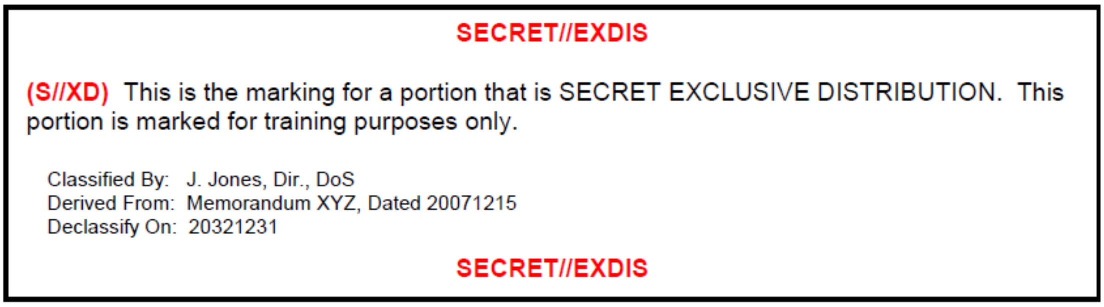
(TS//NF/FISA) This is the marking for a portion which is TOP SECRET, is not releasable to foreign nationals, and contains FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA) information.

Classified By: J. Jones, Mgr., ABC Dept.
Derived From: Memorandum XYZ, Dated 20071215
Declassify On: 20171215

TOP SECRET//NOFORN/FISA

Figure 67. Example of EXDIS Marking

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



SECRET//EXDIS

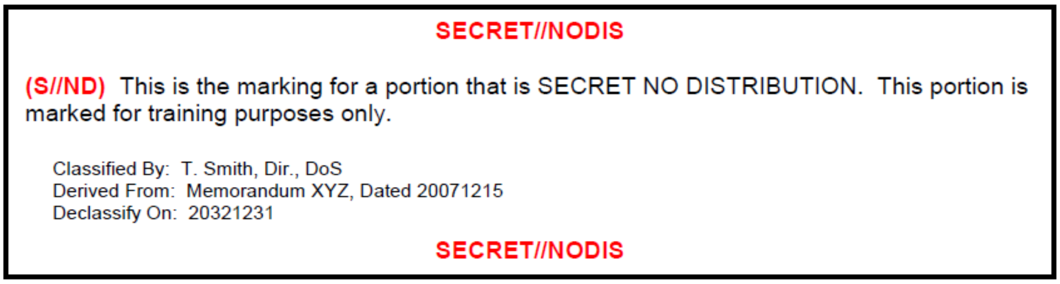
(S//XD) This is the marking for a portion that is SECRET EXCLUSIVE DISTRIBUTION. This portion is marked for training purposes only.

Classified By: J. Jones, Dir., DoS
Derived From: Memorandum XYZ, Dated 20071215
Declassify On: 20321231

SECRET//EXDIS

Figure 68. Example of NODIS Marking

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



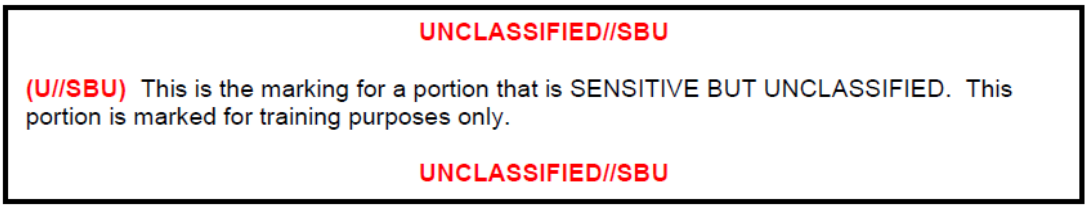
SECRET//NODIS

(S//ND) This is the marking for a portion that is SECRET NO DISTRIBUTION. This portion is marked for training purposes only.

Classified By: T. Smith, Dir., DoS
Derived From: Memorandum XYZ, Dated 20071215
Declassify On: 20321231

SECRET//NODIS

Figure 69. Example of SBU Marking

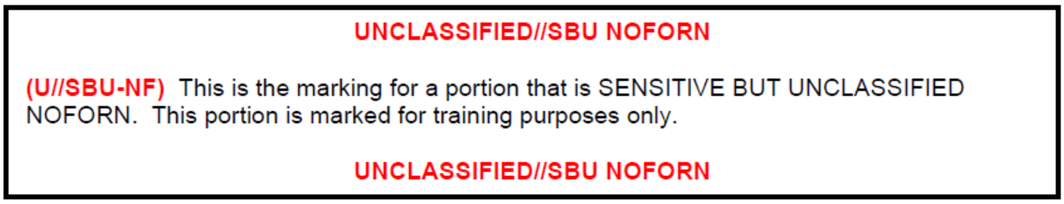


UNCLASSIFIED//SBU

(U//SBU) This is the marking for a portion that is SENSITIVE BUT UNCLASSIFIED. This portion is marked for training purposes only.

UNCLASSIFIED//SBU

Figure 70. Example of SBU-NF Marking



UNCLASSIFIED//SBU NOFORN

(U//SBU-NF) This is the marking for a portion that is SENSITIVE BUT UNCLASSIFIED NOFORN. This portion is marked for training purposes only.

UNCLASSIFIED//SBU NOFORN

⑤ NIST Special Publication 800-53

NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-53r4

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

NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-53r4

April 2013
INCLUDES UPDATES AS OF 01-22-2015

U.S. Department of Commerce
Rebecca M. Blank, Acting Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director

APPENDIX H

INTERNATIONAL INFORMATION SECURITY STANDARDS

SECURITY CONTROL MAPPINGS FOR ISO/IEC 27001 AND 15408

The mapping tables in this appendix provide organizations with a *general* indication of security control coverage with respect to ISO/IEC 27001, *Information technology–Security techniques–Information security management systems–Requirements*[113] and ISO/IEC 15408, *Information technology -- Security techniques -- Evaluation criteria for IT security.*[114] ISO/IEC 27001 may be applied to all types of organizations and specifies requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented information security management system (ISMS) within the context of business risks. NIST Special Publication 800-39 includes guidance on managing risk at the organizational level, mission/business process level, and information system level, is consistent with ISO/IEC 27001, and provides additional implementation detail for the federal government and its contractors. ISO/IEC 15408 (also known as the Common Criteria) provides functionality and assurance requirements for developers of information systems and information system components (i.e., information technology products). Since many of the technical security controls defined in Appendix F are implemented in hardware, software, and firmware components of information systems, organizations can obtain significant benefit from the acquisition and employment of information technology products evaluated against the requirements of ISO/IEC 15408. The use of such products can provide evidence that certain security controls are implemented correctly, operating as intended, and producing the desired effect in satisfying stated security requirements.

Previously, the ISO/IEC 27001 mappings were created by relating the primary security topic identified in each of the Special Publication 800-53 base controls to a similar security topic in the ISO/IEC standard. This methodology resulted in a mapping of security control relationships rather than a mapping of equivalent security control requirements. The ISO/IEC 27001:2013 update provided an opportunity to reassess whether the implementation of a security control from Special Publication 800-53 satisfied the intent of the mapped control from ISO/IEC 27001 and conversely, whether the implementation of a security control from ISO/IEC 27001 satisfied the intent of the mapped control from Special Publication 800-53. To successfully meet the mapping criteria, the implementation of the mapped controls should result in an equivalent information security posture. However, this does not mean that security control equivalency based solely on the mapping tables herein should be assumed by organizations. While the revised security control mappings are more accurate, there is still some degree of subjectivity in the mapping analysis because the mappings are not always one-to-one and may not be completely equivalent. The following examples illustrate some of the mapping issues:

- **Example 1:** Special Publication 800-53 contingency planning and ISO/IEC 27001 business continuity management were deemed to have similar, but not the same, functionality.
- **Example 2:** In some cases, similar topics are addressed in the two security control sets but provide a different context, perspective, or scope. Special Publication 800-53 addresses

[113] ISO/IEC 27001 was published in October 2013 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

[114] ISO/IEC 15408 was published in September 2012 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

information flow control broadly in terms of approved authorizations for controlling access between source and destination objects, whereas ISO/IEC 27001 addresses information flow more narrowly as it applies to interconnected network domains.

- **Example 3:** Security control A.6.1.1, Information Security Roles and Responsibilities, in ISO/IEC 27001 states that "all information security responsibilities shall be defined and allocated" while security control PM-10, Security Authorization Process, in Special Publication 800-53 that is mapped to A.6.1.1, has three distinct parts. The first part states that the organization "designates individuals to fulfill specific roles and responsibilities…" If A.6.1.1 is mapped to PM-10 without providing any additional information, organizations might assume that if they implement A.6.1.1 (i.e., all responsibilities are defined and allocated), then the intent of PM-10 would also be fully satisfied. However, this would not be the case since the other two parts of PM-10 would not have been addressed. To resolve and clarify the security control mappings, when a security control in the right column of Tables H-1 and H-2 does not fully satisfy the intent of the security control in the left column of the tables, the control in the right column is designated with an asterisk (*).

In a few cases, an ISO/IEC 27001 security control could only be directly mapped to a Special Publication 800-53 control enhancement. In such cases, the relevant enhancement is specified in Table H-2 indicating that the corresponding ISO/IEC 27001 control satisfies only the intent of the specified enhancement and does not address the associated base control from Special Publication 800-53 or any other enhancements under that base control. Where no enhancement is specified, the ISO/IEC 27001 control is relevant only to the Special Publication 800-53 base control.

And finally, the security controls from ISO/IEC 27002 were not considered in the mapping analysis since the standard is informative rather than normative.

Table H-1 provides a mapping from the security controls in NIST Special Publication 800-53 to the security controls in ISO/IEC 27001. Please review the introductory text at the beginning of Appendix H before employing the mappings in Table H-1.

TABLE H-1: MAPPING NIST SP 800-53 TO ISO/IEC 27001

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.*
AC-1	Access Control Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.9.1.1, A.12.1.1, A.18.1.1, A.18.2.2
AC-2	Account Management	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6
AC-3	Access Enforcement	A.6.2.2, A.9.1.2, A.9.4.1, A.9.4.4, A.9.4.5 A.13.1.1, A.14.1.2, A.14.1.3, A.18.1.3
AC-4	Information Flow Enforcement	A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3
AC-5	Separation of Duties	A.6.1.2
AC-6	Least Privilege	A.9.1.2, A.9.2.3, A.9.4.4, A.9.4.5
AC-7	Unsuccessful Logon Attempts	A.9.4.2
AC-8	System Use Notification	A.9.4.2
AC-9	Previous Logon (Access) Notification	A.9.4.2
AC-10	Concurrent Session Control	None
AC-11	Session Lock	A.11.2.8, A.11.2.9
AC-12	Session Termination	None
AC-13	**Withdrawn**	---
AC-14	Permitted Actions without Identification or Authentication	None
AC-15	**Withdrawn**	---
AC-16	Security Attributes	None
AC-17	Remote Access	A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2
AC-18	Wireless Access	A.6.2.1, A.13.1.1, A.13.2.1
AC-19	Access Control for Mobile Devices	A.6.2.1, A.11.2.6, A.13.2.1
AC-20	Use of External Information Systems	A.11.2.6, A.13.1.1, A.13.2.1
AC-21	Information Sharing	None
AC-22	Publicly Accessible Content	None
AC-23	Data Mining Protection	None
AC-24	Access Control Decisions	A.9.4.1*
AC-25	Reference Monitor	None
AT-1	Security Awareness and Training Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
AT-2	Security Awareness Training	A.7.2.2, A.12.2.1
AT-3	Role-Based Security Training	A.7.2.2*
AT-4	Security Training Records	None
AT-5	**Withdrawn**	---
AU-1	Audit and Accountability Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
AU-2	Audit Events	None
AU-3	Content of Audit Records	A.12.4.1*
AU-4	Audit Storage Capacity	A.12.1.3
AU-5	Response to Audit Processing Failures	None
AU-6	Audit Review, Analysis, and Reporting	A.12.4.1, A.16.1.2, A.16.1.4
AU-7	Audit Reduction and Report Generation	None
AU-8	Time Stamps	A.12.4.4
AU-9	Protection of Audit Information	A.12.4.2, A.12.4.3, A.18.1.3
AU-10	Non-repudiation	None
AU-11	Audit Record Retention	A.12.4.1, A.16.1.7
AU-12	Audit Generation	A.12.4.1, A.12.4.3

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.*
AU-13	Monitoring for Information Disclosure	None
AU-14	Session Audit	A.12.4.1*
AU-15	Alternate Audit Capability	None
AU-16	Cross-Organizational Auditing	None
CA-1	Security Assessment and Authorization Policies and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
CA-2	Security Assessments	A.14.2.8, A.18.2.2, A.18.2.3
CA-3	System Interconnections	A.13.1.2, A.13.2.1, A.13.2.2
CA-4	**Withdrawn**	---
CA-5	Plan of Action and Milestones	None
CA-6	Security Authorization	None
CA-7	Continuous Monitoring	None
CA-8	Penetration Testing	None
CA-9	Internal System Connections	None
CM-1	Configuration Management Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
CM-2	Baseline Configuration	None
CM-3	Configuration Change Control	A.12.1.2, A.14.2.2, A.14.2.3, A.14.2.4
CM-4	Security Impact Analysis	A.14.2.3
CM-5	Access Restrictions for Change	A.9.2.3, A.9.4.5, A.12.1.2, A.12.1.4, A.12.5.1
CM-6	Configuration Settings	None
CM-7	Least Functionality	A.12.5.1*
CM-8	Information System Component Inventory	A.8.1.1, A.8.1.2
CM-9	Configuration Management Plan	A.6.1.1*
CM-10	Software Usage Restrictions	A.18.1.2
CM-11	User-Installed Software	A.12.5.1, A.12.6.2
CP-1	Contingency Planning Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
CP-2	Contingency Plan	A.6.1.1, A.17.1.1, A.17.2.1
CP-3	Contingency Training	A.7.2.2*
CP-4	Contingency Plan Testing	A.17.1.3
CP-5	**Withdrawn**	---
CP-6	Alternate Storage Site	A.11.1.4, A.17.1.2, A.17.2.1
CP-7	Alternate Processing Site	A.11.1.4, A.17.1.2, A.17.2.1
CP-8	Telecommunications Services	A.11.2.2, A.17.1.2
CP-9	Information System Backup	A.12.3.1, A.17.1.2, A.18.1.3
CP-10	Information System Recovery and Reconstitution	A.17.1.2
CP-11	Alternate Communications Protocols	A.17.1.2*
CP-12	Safe Mode	None
CP-13	Alternative Security Mechanisms	A.17.1.2*
IA-1	Identification and Authentication Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
IA-2	Identification and Authentication (Organizational Users)	A.9.2.1
IA-3	Device Identification and Authentication	None
IA-4	Identifier Management	A.9.2.1
IA-5	Authenticator Management	A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.3
IA-6	Authenticator Feedback	A.9.4.2
IA-7	Cryptographic Module Authentication	A.18.1.5
IA-8	Identification and Authentication (Non-Organizational Users)	A.9.2.1
IA-9	Service Identification and Authentication	None

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.*
IA-10	Adaptive Identification and Authentication	None
IA-11	Re-authentication	None
IR-1	Incident Response Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1 A.18.1.1, A.18.2.2
IR-2	Incident Response Training	A.7.2.2*
IR-3	Incident Response Testing	None
IR-4	Incident Handling	A.16.1.4, A.16.1.5, A.16.1.6
IR-5	Incident Monitoring	None
IR-6	Incident Reporting	A.6.1.3, A.16.1.2
IR-7	Incident Response Assistance	None
IR-8	Incident Response Plan	A.16.1.1
IR-9	Information Spillage Response	None
IR-10	Integrated Information Security Analysis Team	None
MA-1	System Maintenance Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
MA-2	Controlled Maintenance	A.11.2.4*, A.11.2.5*
MA-3	Maintenance Tools	None
MA-4	Nonlocal Maintenance	None
MA-5	Maintenance Personnel	None
MA-6	Timely Maintenance	A.11.2.4
MP-1	Media Protection Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
MP-2	Media Access	A.8.2.3, A.8.3.1, A.11.2.9
MP-3	Media Marking	A.8.2.2
MP-4	Media Storage	A.8.2.3, A.8.3.1, A.11.2.9
MP-5	Media Transport	A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.5, A.11.2.6
MP-6	Media Sanitization	A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7
MP-7	Media Use	A.8.2.3, A.8.3.1
MP-8	Media Downgrading	None
PE-1	Physical and Environmental Protection Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
PE-2	Physical Access Authorizations	A.11.1.2*
PE-3	Physical Access Control	A.11.1.1, A.11.1.2, A.11.1.3
PE-4	Access Control for Transmission Medium	A.11.1.2, A.11.2.3
PE-5	Access Control for Output Devices	A.11.1.2, A.11.1.3
PE-6	Monitoring Physical Access	None
PE-7	**Withdrawn**	---
PE-8	Visitor Access Records	None
PE-9	Power Equipment and Cabling	A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3
PE-10	Emergency Shutoff	A.11.2.2*
PE-11	Emergency Power	A.11.2.2
PE-12	Emergency Lighting	A.11.2.2*
PE-13	Fire Protection	A.11.1.4, A.11.2.1
PE-14	Temperature and Humidity Controls	A.11.1.4, A.11.2.1, A.11.2.2
PE-15	Water Damage Protection	A.11.1.4, A.11.2.1, A.11.2.2
PE-16	Delivery and Removal	A.8.2.3, A.11.1.6, A.11.2.5
PE-17	Alternate Work Site	A.6.2.2, A.11.2.6, A.13.2.1
PE-18	Location of Information System Components	A.8.2.3, A.11.1.4, A.11.2.1
PE-19	Information Leakage	A.11.1.4, A.11.2.1
PE-20	Asset Monitoring and Tracking	A.8.2.3*
PL-1	Security Planning Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
PL-2	System Security Plan	A.14.1.1
PL-3	**Withdrawn**	---
PL-4	Rules of Behavior	A.7.1.2, A.7.2.1, A.8.1.3

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.*
PL-5	**Withdrawn**	---
PL-6	**Withdrawn**	---
PL-7	Security Concept of Operations	A.14.1.1*
PL-8	Information Security Architecture	A.14.1.1*
PL-9	Central Management	None
PS-1	Personnel Security Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
PS-2	Position Risk Designation	None
PS-3	Personnel Screening	A.7.1.1
PS-4	Personnel Termination	A.7.3.1, A.8.1.4
PS-5	Personnel Transfer	A.7.3.1, A.8.1.4
PS-6	Access Agreements	A.7.1.2, A.7.2.1, A.13.2.4
PS-7	Third-Party Personnel Security	A.6.1.1*, A.7.2.1*
PS-8	Personnel Sanctions	A.7.2.3
RA-1	Risk Assessment Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
RA-2	Security Categorization	A.8.2.1
RA-3	Risk Assessment	A.12.6.1*
RA-4	**Withdrawn**	---
RA-5	Vulnerability Scanning	A.12.6.1*
RA-6	Technical Surveillance Countermeasures Survey	None
SA-1	System and Services Acquisition Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
SA-2	Allocation of Resources	None
SA-3	System Development Life Cycle	A.6.1.1, A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.6
SA-4	Acquisition Process	A.14.1.1, A.14.2.7, A.14.2.9, A.15.1.2
SA-5	Information System Documentation	A.12.1.1*
SA-6	**Withdrawn**	---
SA-7	**Withdrawn**	---
SA-8	Security Engineering Principles	A.14.2.5
SA-9	External Information System Services	A.6.1.1, A.6.1.5, A.7.2.1, A.13.1.2, A.13.2.2, A.15.2.1, A.15.2.2
SA-10	Developer Configuration Management	A.12.1.2, A.14.2.2, A.14.2.4, A.14.2.7
SA-11	Developer Security Testing and Evaluation	A.14.2.7, A.14.2.8
SA-12	Supply Chain Protections	A.14.2.7, A.15.1.1, A.15.1.2, A.15.1.3
SA-13	Trustworthiness	None
SA-14	Criticality Analysis	None
SA-15	Development Process, Standards, and Tools	A.6.1.5, A.14.2.1,
SA-16	Developer-Provided Training	None
SA-17	Developer Security Architecture and Design	A.14.2.1, A.14.2.5
SA-18	Tamper Resistance and Detection	None
SA-19	Component Authenticity	None
SA-20	Customized Development of Critical Components	None
SA-21	Developer Screening	A.7.1.1
SA-22	Unsupported System Components	None
SC-1	System and Communications Protection Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
SC-2	Application Partitioning	None
SC-3	Security Function Isolation	None
SC-4	Information In Shared Resources	None
SC-5	Denial of Service Protection	None
SC-6	Resource Availability	None

NIST SP 800-53 CONTROLS		**ISO/IEC 27001 CONTROLS** *Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.*
SC-7	Boundary Protection	A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.3
SC-8	Transmission Confidentiality and Integrity	A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3
SC-9	**Withdrawn**	---
SC-10	Network Disconnect	A.13.1.1
SC-11	Trusted Path	None
SC-12	Cryptographic Key Establishment and Management	A.10.1.2
SC-13	Cryptographic Protection	A.10.1.1, A.14.1.2, A.14.1.3, A.18.1.5
SC-14	**Withdrawn**	---
SC-15	Collaborative Computing Devices	A.13.2.1*
SC-16	Transmission of Security Attributes	None
SC-17	Public Key Infrastructure Certificates	A.10.1.2
SC-18	Mobile Code	None
SC-19	Voice Over Internet Protocol	None
SC-20	Secure Name/Address Resolution Service (Authoritative Source)	None
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	None
SC-22	Architecture and Provisioning for Name/Address Resolution Service	None
SC-23	Session Authenticity	None
SC-24	Fail in Known State	None
SC-25	Thin Nodes	None
SC-26	Honeypots	None
SC-27	Platform-Independent Applications	None
SC-28	Protection of Information at Rest	A.8.2.3*
SC-29	Heterogeneity	None
SC-30	Concealment and Misdirection	None
SC-31	Covert Channel Analysis	None
SC-32	Information System Partitioning	None
SC-33	**Withdrawn**	---
SC-34	Non-Modifiable Executable Programs	None
SC-35	Honeyclients	None
SC-36	Distributed Processing and Storage	None
SC-37	Out-of-Band Channels	None
SC-38	Operations Security	A.12.x
SC-39	Process Isolation	None
SC-40	Wireless Link Protection	None
SC-41	Port and I/O Device Access	None
SC-42	Sensor Capability and Data	None
SC-43	Usage Restrictions	None
SC-44	Detonation Chambers	None
SI-1	System and Information Integrity Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
SI-2	Flaw Remediation	A.12.6.1, A.14.2.2, A.14.2.3, A.16.1.3
SI-3	Malicious Code Protection	A.12.2.1
SI-4	Information System Monitoring	None
SI-5	Security Alerts, Advisories, and Directives	A.6.1.4*
SI-6	Security Function Verification	None
SI-7	Software, Firmware, and Information Integrity	None
SI-8	Spam Protection	None
SI-9	**Withdrawn**	---

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.*
SI-10	Information Input Validation	None
SI-11	Error Handling	None
SI-12	Information Handling and Retention	None
SI-13	Predictable Failure Prevention	None
SI-14	Non-Persistence	None
SI-15	Information Output Filtering	None
SI-16	Memory Protection	None
SI-17	Fail-Safe Procedures	None
PM-1	Information Security Program Plan	A.5.1.1, A.5.1.2, A.6.1.1, A.18.1.1, A.18.2.2
PM-2	Senior Information Security Officer	A.6.1.1*
PM-3	Information Security Resources	None
PM-4	Plan of Action and Milestones Process	None
PM-5	Information System Inventory	None
PM-6	Information Security Measures of Performance	None
PM-7	Enterprise Architecture	None
PM-8	Critical Infrastructure Plan	None
PM-9	Risk Management Strategy	None
PM-10	Security Authorization Process	A.6.1.1*
PM-11	Mission/Business Process Definition	None
PM-12	Insider Threat Program	None
PM-13	Information Security Workforce	A.7.2.2*
PM-14	Testing, Training, and Monitoring	None
PM-15	Contacts with Security Groups and Associations	A.6.1.4
PM-16	Threat Awareness Program	None

Table H-2 provides a mapping from the security controls in ISO/IEC 27001 to the security controls in Special Publication 800-53.[115] Please review the introductory text at the beginning of Appendix H before employing the mappings in Table H-2.

TABLE H-2: MAPPING ISO/IEC 27001 TO NIST SP 800-53

ISO/IEC 27001 CONTROLS	**NIST SP 800-53 CONTROLS** *Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.*
A.5 Information Security Policies	
A.5.1 Management direction for information security	
A.5.1.1 Policies for information security	All XX-1 controls
A.5.1.2 Review of the policies for information security	All XX-1 controls
A.6 Organization of information security	
A.6.1 Internal organization	
A.6.1.1 Information security roles and responsibilities	All XX-1 controls, CM-9, CP-2,PS-7, SA-3, SA-9, PM- 2, PM-10
A.6.1.2 Segregation of duties	AC-5
A.6.1.3 Contact with authorities	IR-6
A.6.1.4 Contact with special interest groups	SI-5, PM-15
A.6.1.5 Information security in project management	SA-3, SA-9, SA-15
A.6.2 Mobile devices and teleworking	
A.6.2.1 Mobile device policy	AC-17, AC-18, AC-19
A.6.2.2 Teleworking	AC-3, AC-17, PE-17
A.7 Human Resources Security	
A.7.1 Prior to Employment	
A.7.1.1 Screening	PS-3, SA-21
A.7.1.2 Terms and conditions of employment	PL-4, PS-6
A.7.2 During employment	
A.7.2.1 Management responsibilities	PL-4, PS-6, PS-7, SA-9
A.7.2.2 Information security awareness, education, anc training	AT-2, AT-3, CP-3, IR-2, PM-13
A.7.2.3 Disciplinary process	PS-8
A.7.3 Termination and change of employment	
A.7.3.1 Termination or change of employment responsibilities	PS-4, PS-5
A.8 Asset Management	
A.8.1 Responsibility for assets	
A.8.1.1 Inventory of assets	CM-8
A.8.1.2 Ownership of assets	CM-8
A.8.1.3 Acceptable use of assets	PL-4
A.8.1.4 Return of assets	PS-4, PS-5
A.8.2 Information Classification	
A.8.2.1 Classification of information	RA-2
A.8.2.2 Labelling of Information	MP-3
A.8.2.3 Handling of Assets	MP-2, MP-4, MP-5, MP-6, MP-7, PE-16, PE-18, PE- 20, SC-8, SC-28
A.8.3 Media Handling	
A.8.3.1 Management of removable media	MP-2, MP-4, MP-5, MP-6, MP-7
A.8.3.2 Disposal of media	MP-6
A.8.3.3 Physical media transfer	MP-5
A.9 Access Control	

[115] The use of the term *XX-1 controls* in mapping Table H-2 refers to the set of security controls represented by the first control in each family in Appendix F, where *XX* is a placeholder for the two-letter family identifier.

ISO/IEC 27001 CONTROLS	**NIST SP 800-53 CONTROLS** *Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.*
A.9.1 Business requirement of access control	
A.9.1.1 Access control policy	AC-1
A.9.1.2 Access to networks and network services	AC-3, AC-6
A.9.2 User access management	
A.9.2.1 User registration and de-registration	AC-2, IA-2, IA-4, IA-5, IA-8
A.9.2.2 User access provisioning	AC-2
A.9.2.3 Management of privileged access rights	AC-2, AC-3, AC-6, CM-5
A.9.2.4 Management of secret authentication informaion of users	IA-5
A.9.2.5 Review of user access rights	AC-2
A.9.2.6 Removal or adjustment of access rights	AC-2
A.9.3 User responsibilities	
A.9.3.1 Use of secret authentication information	IA-5
A.9.4 System and application access control	
A.9.4.1 Information access restriction	AC-3, AC-24
A.9.4.2 Secure logon procedures	AC-7, AC-8, AC-9, IA-6
A.9.4.3 Password management system	IA-5
A.9.4.4 Use of privileged utility programs	AC-3, AC-6
A.9.4.5 Access control to program source code	AC-3, AC-6, CM-5
A.10 Cryptography	
A.10.1 Cryptographic controls	
A.10.1.1 Policy on the use of cryptographic controls	SC-13
A.10.1.2 Key Management	SC-12, SC-17
A.11 Physical and environmental security	
A.11.1 Secure areas	
A.11.1.1 Physical security perimeter	PE-3*
A.11.1.2 Physical entry controls	PE-2, PE-3, PE-4, PE-5
A.11.1.3 Securing offices, rooms and facilities	PE-3, PE-5
A.11.1.4 Protecting against external and environmental threats	CP-6, CP-7, PE-9, PE-13, PE-14, PE-15, PE-18, PE- 19
A.11.1.5 Working in secure areas	SC-42(3)*
A.11.1.6 Delivery and loading areas	PE-16
A.11.2 Equipment	
A.11.2.1 Equipment siting and protection	PE-9, PE-13, PE-14, PE-15, PE-18, PE-19
A.11.2.2 Supporting utilities	CP-8, PE-9, PE-10, PE-11, PE-12, PE-14, PE-15
A.11.2.3 Cabling security	PE-4, PE-9
A.11.2.4 Equipment maintenance	MA-2, MA-6
A.11.2.5 Removal of assets	MA-2, MP-5, PE-16
A.11.2.6 Security of equipment and assets off-premises	AC-19, AC-20, MP-5, PE-17
A.11.2.7 Secure disposal or reuse of equipment	MP-6
A.11.2.8 Unattended user equipment	AC-11
A.11.2.9 Clear desk and clear screen policy	AC-11, MP-2, MP-4
A.12 Operations security	
A.12.1 Operational procedures and responsibilities	
A.12.1.1 Documented operating procedures	All XX-1 controls, SA-5
A.12.1.2 Change management	CM-3, CM-5, SA-10
A.12.1.3 Capacity management	AU-4, CP-2(2), SC-5(2)
A.12.1.4 Separation of development, testing, and operational environments	CM-4(1)*, CM-5*
A.12.2 Protection from malware	
A.12.2.1 Controls against malware	AT-2, SI-3

ISO/IEC 27001 CONTROLS	NIST SP 800-53 CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.*
A.12.3 Backup	
A.12.3.1 Information backup	CP-9
A.12.4 Logging and monitoring	
A.12.4.1 Event logging	AU-3, AU-6, AU-11, AU-12, AU-14
A.12.4.2 Protection of log information	AU-9
A.12.4.3 Administrator and operator logs	AU-9, AU-12
A.12.4.4 Clock synchronization	AU-8
A.12.5 Control of operational software	
A.12.5.1 Installation of software on operational systems	CM-5, CM-7(4), CM-7(5), CM-11
A.12.6 Technical vulnerability management	
A.12.6.1 Management of technical vulnerabilities	RA-3, RA-5, SI-2, SI-5
A.12.6.2 Restrictions on software installation	CM-11
A.12.7 Information systems audit considerations	
A.12.7.1 Information systems audit controls	AU-5*
A.13 Communications security	
A.13.1 Network security management	
A.13.1.1 Network controls	AC-3, AC-17, AC-18, AC-20, SC-7, SC-8, SC-10
A.13.1.2 Security of network services	CA-3, SA-9
A.13.1.3 Segregation in networks	AC-4, SC-7
A.13.2 Information transfer	
A.13.2.1 Information transfer policies and procedures	AC-4, AC-17, AC-18, AC-19, AC-20, CA-3, PE-17, SC-7, SC-8, SC-15
A.13.2.2 Agreements on information transfer	CA-3, PS-6, SA-9
A.13.2.3 Electronic messaging	SC-8
A.13.2.4 Confidentiality or nondisclosure agreements	PS-6
A.14 System acquisition, development and maintenance	
A.14.1 Security requirements of information systems	
A.14.1.1 Information security requirements analysis and specification	PL-2, PL-7, PL-8, SA-3, SA-4
A.14.1.2 Securing application services on public networks	AC-3, AC-4, AC-17, SC-8, SC-13
A.14.1.3 Protecting application services transactions	AC-3, AC-4, SC-7, SC-8, SC-13
A.14.2 Security in development and support processes	
A.14.2.1 Secure development policy	SA-3, SA-15, SA-17
A.14.2.2 System change control procedures	CM-3, SA-10, SI-2
A.14.2.3 Technical review of applications after operaing platform changes	CM-3, CM-4, SI-2
A.14.2.4 Restrictions on changes to software packages	CM-3, SA-10
A.14.2.5 Secure system engineering principles	SA-8
A.14.2.6 Secure development environment	SA-3*
A.14.2.7 Outsourced development	SA-4, SA-10, SA-11, SA-12, SA-15
A.14.2.8 System security testing	CA-2, SA-11
A.14.2.9 System acceptance testing	SA-4, SA-12(7)
A.14.3 Test data	
A.14.3.1 Protection of test data	SA-15(9)*
A.15 Supplier Relationships	
A.15.1 Information security in supplier relationships	
A.15.1.1 Information security policy for supplier relationships	SA-12
A.15.1.2 Address security within supplier agreements	SA-4, SA-12

ISO/IEC 27001 CONTROLS	**NIST SP 800-53 CONTROLS** *Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.*
A.15.1.3 Information and communication technology supply chain	SA-12
A.15.2 Supplier service delivery management	
A.15.2.1 Monitoring and review of supplier services	SA-9
A.15.2.2 Managing changes to supplier services	SA-9
A.16 Information security incident management	
A.16.1 Managing of information security incidents and improvements	
A.16.1.1 Responsibilities and procedures	IR-8
A.16.1.2 Reporting information security events	AU-6, IR-6
A.16.1.3 Reporting information security weaknesses	SI-2
A.16.1.4 Assessment of and decision on information security events	AU-6, IR-4
A.16.1.5 Response to information security incidents	IR-4
A.16.1.6 Learning from information security incidents	IR-4
A.16.1.7 Collection of evidence	AU-4*, AU-9*, AU-10(3)*, AU-11*
A.17 Information security aspects of business continuity management	
A.17.1 Information security continuity	
A.17.1.1 Planning information security continuity	CP-2
A.17.1.2 Implementing information security continuity	CP-6, CP-7, CP-8, CP-9, CP-10, CP-11, CP-13
A.17.1.3 Verify, review, and evaluate information security continuity	CP-4
A.17.2 Redundancies	
A.17.2.1 Availability of information processing facilities	CP-2,CP-6, CP-7
A.18 Compliance	
A.18.1 Compliance with legal and contractual requirements	
A.18.1.1 Identification of applicable legislation and contractual requirements	All XX-1 controls
A.18.1.2 Intellectual property rights	CM-10
A.18.1.3 Protection of records	AC-3, AC-23, AU-9, AU-10, CP-9, SC-8, SC-8(1), SC-13, SC-28, SC-28(1)
A.18.1.4 Privacy and protection of personal information	Appendix J Privacy controls
A.18.1.5 Regulation of cryptographic controls	IA-7, SC-12, SC-13, SC-17
A.18.2 **Information security reviews**	
A.18.2.1 Independent review of information security	CA-2(1), SA-11(3)
A.18.2.2 Compliance with security policies and standards	All XX-1 controls, CA-2
A.18.2.3 Technical compliance review	CA-2

Note: The content of Table H-3, the mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the security controls in Special Publication 800-53, is unaffected by the changes above.

Table H-3 provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the security controls in Special Publication 800-53. The table represents an *informal* correspondence between security requirements and security controls (i.e., the table is not intended to determine whether the ISO/IEC 15408 security requirements are fully, partially, or not satisfied by the associated security controls). However, the table can serve as a beneficial starting point for further correspondence analysis. Organizations are cautioned that satisfying ISO/IEC 15408 security requirements for an particular evaluated and validated information technology product as represented by the presence of certain security controls from Appendix F, does not imply that such requirements have been satisfied throughout the entire information system (which may consist of multiple, integrated individual component products). Additional information explaining the specific mappings that appear in Table H-3 is available at the National Information Assurance Partnership (NIAP) website at: http://www.niap-ccevs.org.

TABLE H-3: MAPPING ISO/IEC 15408 TO NIST SP 800-53

ISO/IEC 15408 REQUIREMENTS		**NIST SP 800-53 CONTROLS**	
Functional Requirements			
FAU_ARP.1	**Security Audit Automatic Response** Security Alarms	AU-5	**Response to Audit Processing Failures**
		AU-5(1)	**Response to Audit Processing Failures** *Audit Storage Capacity*
		AU-5(2)	**Response to Audit Processing Failures** *Real-Time Alerts*
		AU-5(3)	**Response to Audit Processing Failures** *Configurable Traffic Volume Thresholds*
		AU-5(4)	**Response to Audit Processing Failures** *Shutdown on Failure*
		PE-6(2)	**Monitoring Physical Access** *Automated Intrusion Recognition / Responses*
		SI-3	**Malicious Code Protection**
		SI-3(8)	**Malicious Code Protection** *Detect Unauthorized Commands*
		SI-4(5)	**Information System Monitoring** *System-Generated Alerts*
		SI-4(7)	**Information Systems Monitoring** *Automated Response to Suspicious Events*
		SI-4(22)	**Information Systems Monitoring** *Unauthorized Network Services*
		SI-7(2)	**Software, Firmware, and Information Integrity** *Automated Notifications of Integrity Violations*
		SI-7(5)	**Software, Firmware, and Information Integrity** *Automated Response to Integrity Violations*
		SI-7(8)	**Software, Firmware, and Information Integrity** *Auditing Capability for Significant Events*
FAU_GEN.1	**Security Audit Data Generation** Audit Data Generation	AU-2	**Audit Events**
		AU-3	**Content of Audit Records**
		AU-3(1)	**Content of Audit Records** *Additional Audit Information*
		AU-12	**Audit Generation**

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
FAU_GEN.2	**Security Audit Data Generation** User Identity Association	AU-3	**Content of Audit Records**
FAU_SAA.1	**Security Audit Analysis** Potential Violation Analysis	SI-4	**Information System Monitoring**
FAU_SAA.2	**Security Audit Analysis** Profile-Based Anomaly Detection	AC-2(12)	**Account Management** *Account Monitoring / Atypical Usage*
		SI-4	**Information System Monitoring**
FAU_SAA.3	**Security Audit Analysis** Simple Attack Heuristics	SI-3(7)	**Malicious Code Protection** *Non Signature-Based Protection*
		SI-4	**Information System Monitoring**
FAU_SAA.4	**Security Audit Analysis** Complex Attack Heuristics	SI-3(7)	**Malicious Code Protection** *Non Signature-Based Protection*
		SI-4	**Information System Monitoring**
FAU_SAR.1	**Security Audit Review** Audit Review	AU-7	**Audit Reduction and Report Generation**
FAU_SAR.2	**Security Audit Review** Restricted Audit Review	AU-9(6)	**Protection of Audit Information** *Read Only Access*
FAU_SAR.3	**Security Audit Review** Selectable Audit Review	AU-7	**Audit Reduction and Report Generation**
		AU-7(1)	**Audit Reduction and Report Generation** *Automatic Processing*
		AU-7(2)	**Audit Reduction and Report Generation** *Automatic Sort and Search*
FAU_SEL.1	**Security Audit Event Selection** Selective Audit	AU-12	**Audit Generation**
FAU_STG.1	**Security Audit Event Storage** Protected Audit Trail Storage	AU-9	**Protection of Audit Information**
FAU_STG.2	**Security Audit Event Storage** Guarantees of Audit Data Availability	AU-9	**Protection of Audit Information** *Alternate audit capability*
FAU_STG.3	**Security Audit Event Storage** Action In Case of Possible Audit Data Loss	AU-5	**Response to Audit Processing Failures**
		AU-5(1)	**Response to Audit Processing Failures** *Audit Storage Capacity*
		AU-5(2)	**Response To Audit Processing Failures** *Real-Time Alerts*
		AU-5(4)	**Response To Audit Processing Failures** *Shutdown on Failure*
FAU_STG.4	**Security Audit Event Storage** Prevention of Audit Data Loss	AU-4	**Audit Storage Capacity**
		AU-5	**Response to Audit Processing Failures**
		AU-5(2)	**Response To Audit Processing Failures** *Real-Time Alerts*
		AU-5(4)	**Response To Audit Processing Failures** *Shutdown on Failure*
FCO_NRO.1	**Non-Repudiation of Origin** Selective Proof of Origin	AU-10	**Non-Repudiation**
		AU-10(1)	**Non-Repudiation** *Association Of Identities*
		AU-10(2)	**Non-Repudiation** *Validate Binding of Information Producer Identity*

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
FCO_NRO.2	**Non-Repudiation of Origin** Enforced Proof of Origin	AU-10	**Non-Repudiation**
		AU-10(1)	**Non-Repudiation** *Association Of Identities*
		AU-10(2)	**Non-Repudiation** *Validate Binding of Information Producer Identity*
FCO_NRR.1	**Non-Repudiation of Receipt** Selective Proof of Receipt	AU-10	**Non-Repudiation**
		AU-10(1)	**Non-Repudiation** *Association Of Identities*
		AU-10(2)	**Non-Repudiation** *Validate Binding of Information Producer Identity*
FCO_NRR.2	**Non-Repudiation of Receipt** Enforced Proof of Receipt	AU-10	**Non-Repudiation**
		AU-10(1)	**Non-Repudiation** *Association Of Identities*
		AU-10(2)	**Non-Repudiation** *Validate Binding of Information Producer Identity*
FCS_CKM.1	**Cryptographic Key Management** Cryptographic Key Generation	SC-12	**Cryptographic Key Establishment and Management**
FCS_CKM.2	**Cryptographic Key Management** Cryptographic Key Distribution	SC-12	**Cryptographic Key Establishment and Management**
FCS_CKM.3	**Cryptographic Key Management** Cryptographic Key Access	SC-12	**Cryptographic Key Establishment and Management**
FCS_CKM.4	**Cryptographic Key Management** Cryptographic Key Destruction	SC-12	**Cryptographic Key Establishment and Management**
FCS_COP.1	**Cryptographic Operation** Cryptographic Operation	SC-13	**Cryptographic Protection**
FDP_ACC.1	**Access Control Policy** Subset Access Control	AC-3	**Access Enforcement**
		AC-3(3)	**Access Enforcement** *Mandatory Access Control*
		AC-3(4)	**Access Enforcement** *Discretionary Access Control*
		AC-3(7)	**Access Enforcement** *Role-Based Access Control*
FDP_ACC.2	**Access Control Policy** Complete Access Control	AC-3	**Access Enforcement**
		AC-3(3)	**Access Enforcement** *Mandatory Access Control*
		AC-3(4)	**Access Enforcement** *Discretionary Access Control*
		AC-3(7)	**Access Enforcement** *Role-Based Access Control*
FDP_ACF.1	**Access Control Functions** Security Attribute Based Access Control	AC-3	**Access Enforcement**
		AC-3(3)	**Access Enforcement** *Mandatory Access Control*
		AC-3(4)	**Access Enforcement** *Discretionary Access Control*
		AC-3(7)	**Access Enforcement** *Role-Based Access Control*
		AC-16	**Security Attributes**

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
		SC-16	**Transmission of Security Attributes**
FDP_DAU.1	**Data Authentication** Basic Data Authentication	SI-7	**Software, Firmware, and Information Integrity**
		SI-7(1)	**Software, Firmware, and Information Integrity** *Integrity Checks*
		SI-7(6)	**Software, Firmware, And Information Integrity** *Cryptographic Protection*
		SI-10	**Information Input Validation**
FDP_DAU.2	**Data Authentication** Data Authentication With Identity of Guarantor	SI-7	**Software, Firmware, and Information Integrity**
		SI-7(1)	**Software, Firmware, and Information Integrity** *Integrity Checks*
		SI-7(6)	**Software, Firmware, And Information Integrity** *Cryptographic Protection*
		SI-10	**Information Input Validation**
FDP_ETC.1	**Export from the TOE** Export of User Data without Security Attributes	No Mapping.	
FDP_ETC.2	**Export from the TOE** Export of User Data with Security Attributes	AC-4(18)	**Information Flow Enforcement** *Security Attribute Binding*
		AC-16	**Security Attributes**
		AC-16(5)	**Security Attributes** *Attribute Displays for Output Devices*
		SC-16	**Transmission of Security Attributes**
FDP_IFC.1	**Information Flow Control Policy** Subset Information Flow Control	AC-3	**Access Enforcement**
		AC-3(3)	**Access Enforcement** *Mandatory Access Control*
		AC-4	**Information Flow Enforcement**
		AC-4(1)	**Information Flow Enforcement** *Object Security Attributes*
FDP_IFC.2	**Information Flow Control Policy** Complete Information Flow Control	AC-3	**Access Enforcement**
		AC-3(3)	**Access Enforcement** *Mandatory Access Control*
		AC-4	**Information Flow Enforcement**
FDP_IFF.1	**Information Flow Control Functions** Simple Security Attributes	AC-3	**Access Enforcement**
		AC-3(3)	**Access Enforcement** *Mandatory Access Control*
		AC-4	**Information Flow Enforcement**
		AC-4(1)	**Information Flow Enforcement** *Object Security Attributes*
		AC-4(2)	**Information Flow Enforcement** *Processing Domains*
		AC-4(7)	**Information Flow Enforcement** *One-Way Flow Mechanisms*
		AC-16	**Security Attributes**
		SC-7	**Boundary Protection**

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
FDP_IFF.2	**Information Flow Control Functions** Hierarchical Security Attributes	AC-3	**Access Enforcement**
		AC-3(3)	**Access Enforcement** *Mandatory Access Control*
		AC-4(1)	**Information Flow Enforcement** *Object Security Attributes*
		AC-16	**Security Attributes**
FDP_IFF.3	**Information Flow Control Functions** Limited Illicit Information Flows	SC-31	**Covert Channel Analysis**
		SC-31(2)	**Covert Channel Analysis** *Maximum Bandwidth*
FDP_IFF.4	**Information Flow Control Functions** Partial Elimination of Illicit Information Flows	SC-31	**Covert Channel Analysis**
		SC-31(2)	**Covert Channel Analysis** *Maximum Bandwidth*
FDP_IFF.5	**Information Flow Control Functions** No Illicit Information Flows	SC-31	**Covert Channel Analysis**
		SC-31(2)	**Covert Channel Analysis** *Maximum Bandwidth*
FDP_IFF.6	**Information Flow Control Functions** Illicit Information Flow Monitoring	SC-31	**Covert Channel Analysis**
		SI-4(18)	**Information System Monitoring** *Analyze Traffic / Covert Exfiltration*
FDP_ITC.1	**Import from Outside of the TOE** Import of User Data without Security Attributes	AC-4(9)	**Information Flow Enforcement** *Human Reviews*
		AC-4(12)	**Information Flow Enforcement** *Data Type Identifiers*
FDP_ITC.2	**Import from Outside of the TOE** Import of User Data with Security Attributes	AC-4(18)	**Information Flow Enforcement** *Security Attribute Binding*
		AC-16	**Security Attributes**
		SC-16	**Transmission of Security Attributes**
FDP_ITT.1	**Internal TOE Transfer** Basic Internal Transfer Protection	SC-8	**Transmission Confidentiality and Integrity**
		SC-8(1)	**Transmission Confidentiality and Integrity** *Cryptographic or Alternate Physical Protection*
		SC-5	**Denial of Service Protection**
FDP_ITT.2	**Internal TOE Transfer** Transmission Separation by Attribute	SC-8	**Transmission Confidentiality and Integrity**
		SC-8(1)	**Transmission Confidentiality and Integrity** *Cryptographic or Alternate Physical Protection*
		SC-5	**Denial of Service Protection**
		AC-4(21)	**Information Flow Enforcement** *Physical / Logical Separation of Information Flows*
FDP_ITT.3	**Internal TOE Transfer** Integrity Monitoring	SI-7	**Software, Firmware, and Information Integrity**
		SI-7(1)	**Software, Firmware, and Information Integrity** *Integrity Checks*
		SC-8(1)	**Transmission Integrity** *Cryptographic or Alternate Physical Protection*
		SI-7(5)	**Software, Firmware, and Information Integrity** *Automated Response to Integrity Violations*

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
FDP_ITT.4	**Internal TOE Transfer** Attribute-Based Integrity Monitoring	SI-7	**Software, Firmware, and Information Integrity**
		SI-7(1)	**Software, Firmware, and Information Integrity** *Integrity Checks*
		SC-8(1)	**Transmission Integrity** *Cryptographic or Alternate Physical Protection*
		AC-4(21)	**Information Flow Enforcement** *Physical / Logical Separation of Information Flows*
		SI-7(5)	**Software, Firmware, and Information Integrity** *Automated Response to Integrity Violations*
FDP_RIP.1	**Residual Information Protection** Subset Residual Information Protection	SC-4	**Information in Shared Resources**
FDP_RIP.2	**Residual Information Protection** Full Residual Information Protection	SC-4	**Information in Shared Resources**
FDP_ROL.1	**Rollback** Basic Rollback	CP-10(2)	**Information System Recovery and Reconstitution** *Transaction Recovery*
FDP_ROL.2	**Rollback** Advanced Rollback	CP-10(2)	**Information System Recovery and Reconstitution** *Transaction Recovery*
FDP_SDI.1	**Stored Data Integrity** Stored Data Integrity Monitoring	SI-7	**Software, Firmware, and Information Integrity**
		SI-7(1)	**Software, Firmware, and Information Integrity** *Integrity Scans*
FDP_SDI.2	**Stored Data Integrity** Stored Data Integrity Monitoring and Action	SI-7	**Software, Firmware, and Information Integrity**
		SI-7(1)	**Software, Firmware, and Information Integrity** *Integrity Scans*
		SI-7(5)	**Software, Firmware, and Information Integrity** *Automated Response to Integrity Violations*
FDP_UCT.1	**Inter-TSF User Data Confidentiality Transfer Protection** Basic Data Exchange Confidentiality	SC-8	**Transmission Confidentiality and Integrity**
		SC-8(1)	**Transmission Confidentiality and Integrity** *Cryptographic or Alternate Physical Protection*
FDP_UIT.1	**Inter-TSF User Data Integrity Transfer Protection** Data Exchange Integrity	SC-8	**Transmission Confidentiality and Integrity**
		SC-8(1)	**Transmission Confidentiality and Integrity** *Cryptographic or Alternate Physical Protection*
		SI-7	**Software, Firmware, and Information Integrity**
		SI-7(6)	**Software, Firmware, and Information Integrity** *Cryptographic Protection*
FDP_UIT.2	**Inter-TSF User Data Integrity Transfer Protection** Source Data Exchange Recovery	No Mapping.	

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
FDP_UIT.3	**Inter-TSF User Data Integrity Transfer Protection** Destination Data Exchange Recovery	No Mapping.	
FIA_AFL.1	**Authentication Failure** Authentication Failure Handling	AC-7	**Unsuccessful Logon Attempts**
FIA_ATD.1	**User Attribute Definition** User Attribute Definition	AC-2	**Account Management**
		IA-2	**Identification and Authentication (Organizational Users)**
FIA_SOS.1	**Specification of Secrets** Verification of Secrets	IA-5	**Authenticator Management**
		IA-5(1)	**Authenticator Management** Password-Based Authentication
		IA-5(12)	**Authenticator Management** Biometric Authentication
FIA_SOS.2	**Specification of Secrets** TSF Generation of Secrets	IA-5	**Authenticator Management**
		IA-5(1)	**Authenticator Management** Password-Based Authentication
		IA-5(12)	**Authenticator Management** Biometric Authentication
FIA_UAU.1	**User Authentication** Timing of Authentication	AC-14	**Permitted Actions without Identification or Authentication**
		IA-2	**Identification and Authentication (Organizational Users)**
		IA-8	**Identification and Authentication (Non-Organizational Users)**
FIA_UAU.2	**User Authentication** User Authentication Before Any Action	AC-14	**Permitted Actions without Identification or Authentication**
		IA-2	**Identification and Authentication (Organizational Users)**
		IA-8	**Identification and Authentication (Non-Organizational Users)**
FIA_UAU.3	**User Authentication** Unforgeable Authentication	IA-2(8)	**Identification and Authentication (Organizational Users)** *Network Access To Privileged Accounts - Replay Resistant*
		IA-2(9)	**Identification and Authentication (Organizational Users)** *Network Access To Non-Privileged Accounts - Replay Resistant*
FIA_UAU.4	**User Authentication** Single-Use Authentication Mechanisms	IA-2(8)	**Identification and Authentication (Organizational Users)** *Network Access To Privileged Accounts - Replay Resistant*
		IA-2(9)	**Identification and Authentication (Organizational Users)** *Network Access To Non-Privileged Accounts - Replay Resistant*
FIA_UAU.5	**User Authentication** Multiple Authentication Mechanisms	IA-2(1)	**Identification and Authentication (Organizational Users)** Network Access To Privileged Accounts
		IA-2(2)	**Identification and Authentication (Organizational Users)** Network Access To Non-Privileged Accounts

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
		IA-2(3)	**Identification and Authentication (Organizational Users)** Local Access To Privileged Accounts
		IA-2(4)	**Identification and Authentication (Organizational Users)** Local Access To Non-Privileged Accounts
		IA-2(6)	**Identification and Authentication (Organizational Users)** Network Access To Privileged Accounts - Separate Device
		IA-2(7)	**Identification and Authentication (Organizational Users)** Network Access To Non-Privileged Accounts - Separate Device
		IA-2(11)	**Identification and Authentication (Organizational Users)** Remote Access - Separate Device
FIA_UAU.6	**User Authentication** Re-Authenticating	IA-11	**Re-authentication**
FIA_UAU.7	**User Authentication** Protected Authentication Feedback	IA-6	**Authenticator Feedback**
FIA_UID.1	**User Identification** Timing of Identification	AC-14	**Permitted Actions without Identification or Authentication**
		IA-2	**Identification and Authentication (Organizational Users)**
		IA-8	**Identification and Authentication (Non-Organizational Users)**
FIA_UID.2	**User Identification** User Identification Before Any Action	AC-14	**Permitted Actions without Identification or Authentication**
		IA-2	**Identification and Authentication (Organizational Users)**
		IA-8	**Identification and Authentication (Non-Organizational Users)**
FIA_USB.1	**User-Subject Binding** User-Subject Binding	AC-16(3)	**Security Attributes** Maintenance Of Attribute Associations By Information System
FMT_MOF.1	**Management of Functions in TSF** Management of Security Functions Behavior	AC-3(7)	**Access Enforcement** Role-Based Access Control
		AC-6	**Least Privilege**
		AC-6(1)	**Least Privilege** Authorize Access To Security Functions
FMT_MSA.1	**Management of Security Attributes** Management of Security Attributes	AC-6	**Least Privilege**
		AC-6(1)	**Least Privilege** Authorize Access To Security Functions
		AC-16(2)	**Security Attributes** Attribute Value Changes By Authorized Individuals
		AC-16(4)	**Security Attributes** Association of Attributes By Authorized Individuals
		AC-16(10)	**Security Attributes** Attribute Configuration By Authorized Individuals

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
FMT_MSA.2	**Management of Security Attributes** Secure Security Attributes	AC-16	**Security Attributes**
		CM-6	**Configuration Settings**
		SI-10	**Information Input Validation**
FMT_MSA.3	**Management of Security Attributes** Static Attribute Initialization	No Mapping.	
FMT_MSA.4	**Management of Security Attributes** Security Attribute Value Inheritance	No Mapping.	
FMT_MTD.1	**Management of TSF Data** Management of TSF Data	AC-3(7)	**Access Enforcement** Role-Based Access Control
		AC-6	**Least Privilege**
		AC-6(1)	**Least Privilege** Authorize Access To Security Functions
		AU-6(7)	**Audit Review, Analysis, and Reporting** Permitted Actions
		AU-9(4)	**Protection of Audit Information** Access By Subset of Privileged Users
FMT_MTD.2	**Management of TSF Data** Management of Limits on TSF Data	AC-3(7)	**Access Enforcement** Role-based Access Control
		AC-6	**Least Privilege**
		AC-6(1)	**Least Privilege** Authorize Access To Security Functions
FMT_MTD.3	**Management of TSF Data** Secure TSF Data	SI-10	**Information Input Validation**
FMT_REV.1	**Revocation** Revocation	AC-3(7)	**Access Enforcement** Rose-based Access Control
		AC-3(8)	**Access Enforcement** Revocation Of Access Authorizations
		AC-6	**Least Privilege**
		AC-6(1)	**Least Privilege** Authorize Access To Security Functions
FMT_SAE.1	**Security Attribute Expiration** Time-Limited Authorization	AC-3(7)	**Access Enforcement** Role-based Access Control
		AC-6	**Least Privilege**
		AC-6(1)	**Least Privilege** Authorize Access To Security Functions
FMT_SMF.1	**Specification of Management Functions** Specification of Management Functions	No Mapping.	
FMT_SMR.1	**Security Management Roles** Security Roles	AC-2(7)	**Account Management** Role-based schemes
		AC-3(7)	**Access Enforcement** Role-Based Access Control
		AC-5	**Separation of Duties**
		AC-6	**Least Privilege**
FMT_SMR.2	**Security Management Roles** Restrictions on Security Roles	AC-2(7)	**Account Management** Role-based schemes
		AC-3(7)	**Access Enforcement** Role-Based Access Control
		AC-5	**Separation of Duties**

ISO/IEC 15408 REQUIREMENTS		**NIST SP 800-53 CONTROLS**	
		AC-6	**Least Privilege**
FMT_SMR.3	**Security Management Roles** Assuming Roles	AC-6(1)	**Least Privilege** Authorized Access to Security Functions
		AC-6(2)	**Least Privilege** Non-Privileged Access For Nonsecurity Functions
FPR_ANO.1	**Anonymity** Anonymity	No Mapping.	
FPR_ANO.2	**Anonymity** Anonymity Without Soliciting Information	No Mapping.	
FPR_PSE.1	**Pseudonymity** Pseudonymity	No Mapping.	
FPR_PSE.2	**Pseudonymity** Reversible Pseudonymity	No Mapping.	
FPR_PSE.3	**Pseudonymity** Alias Pseudonymity	No Mapping.	
FPR_UNL.1	**Unlinkability** Unlinkability	No Mapping.	
FPR_UNO.1	**Unobservability** Unobservability	No Mapping.	
FPR_UNO.2	**Unobservability** Allocation of Information Impacting Unobservability	No Mapping.	
FPR_UNO.3	**Unobservability** Unobservability Without Soliciting Information	No Mapping.	
FPR_UNO.4	**Unobservability** Authorized User Observability	No Mapping.	
FPT_FLS.1	**Fail Secure** Failure with Preservation of Secure State	SC-7(18)	**Boundary Protection** Fail Secure
		SC-24	**Fail in Known State**
FPT_ITA.1	**Availability of Exported TSF Data** Inter-TSF Availability within a Defined Availability Metric	CP-10	**Information System Recovery And Reconstitution** Restore Within Time Period
		SC-5	**Denial of Service Protection**
		SC-5(2)	**Denial of Service Protection** Excess Capacity/Bandwidth/Redundancy
		SC-5(3)	**Denial of Service Protection** Detection/Monitoring
FPT_ITC.1	**Confidentiality of Exported TSF Data** Inter-TSF Confidentiality During Transmission	SC-8	**Transmission Confidentiality and Integrity**
		SC-8(1)	**Transmission Confidentiality and Integrity** Cryptographic Or Alternate Physical Protection
FPT_ITI.1	**Integrity of Exported TSF Data** Inter-TSF Detection of Modification	SC-8	**Transmission Confidentiality and Integrity**
		SC-8(1)	**Transmission Confidentiality and Integrity** Cryptographic Or Alternate Physical Protection
		SI-7	**Software, Firmware, and Information Integrity**
		SI-7(1)	**Software, Firmware, and Information Integrity** Integrity Scans

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
		SI-7(5)	**Software, Firmware, and Information Integrity** Automated Response to Integrity Violations
		SI-7(6)	**Software, Firmware, and Information Integrity** Cryptographic Protection
FPT_ITI.2	**Integrity of Exported TSF Data** Inter-TSF Detection and Correction of Modification	SC-8	**Transmission Confidentiality and Integrity**
		SC-8(1)	**Transmission Confidentiality and Integrity** Cryptographic Or Alternate Physical Protection
		SI-7	**Software, Firmware, and Information Integrity**
		SI-7(1)	**Software, Firmware, and Information Integrity** Integrity Scans
		SI-7(5)	**Software, Firmware, and Information Integrity** Automated Response to Integrity Violations
		SI-7(6)	**Software, Firmware, and Information Integrity** Cryptographic Protection
FPT_ITT.1	**Internal TOE TSF Data Transfer** Basic Internal TSF Data Transfer Protection	SC-8	**Transmission Confidentiality and Integrity**
		SC-8(1)	**Transmission Confidentiality and Integrity** Cryptographic Or Alternate Physical Protection
FPT_ITT.2	**Internal TOE TSF Data Transfer** TSF Data Transfer Separation	AC-4(21)	**Information Flow Enforcement** Physical / Logical Separation Of Information Flows
		SC-8	**Transmission Confidentiality and Integrity**
		SC-8(1)	**Transmission Confidentiality and Integrity** Cryptographic Or Alternate Physical Protection
FPT_ITT.3	**Internal TOE TSF Data Transfer** TSF Data Integrity Monitoring	SI-7	**Software, Firmware, and Information Integrity**
		SI-7(1)	**Software, Firmware, and Information Integrity** Integrity Scans
		SI-7(5)	**Software, Firmware, and Information Integrity** Automated Response to Integrity Violations
		SI-7(6)	**Software, Firmware, and Information Integrity** Cryptographic Protection
FPT_PHP.1	**TSF Physical Protection** Passive Detection of Physical Attack	PE-3(5)	**Physical Access Control** Tamper Protection
		PE-6(2)	**Monitoring Physical Access** Automated Intrusion Recognition / Responses
		SA-18	**Tamper Resistance and Detection**
FPT_PHP.2	**TSF Physical Protection** Notification of Physical Attack	PE-3(5)	**Physical Access Control** Tamper Protection
		PE-6(2)	**Monitoring Physical Access** Automated Intrusion Recognition / Responses
		SA-18	**Tamper Resistance and Detection**
FPT_PHP.3	**TSF Physical Protection** Resistance to Physical Attack	PE-3(5)	**Physical Access Control** Tamper Protection

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
		SA-18	**Tamper Resistance and Detection**
FPT_RCV.1	**Trusted Recovery** Manual Recovery	CP-10	**Information System Recovery and Reconstitution**
		CP-12	**Safe Mode**
FPT_RCV.2	**Trusted Recovery** Automated Recovery	CP-10	**Information System Recovery and Reconstitution**
		CP-12	**Safe Mode**
FPT_RCV.3	**Trusted Recovery** Automated Recovery Without Undue Loss	CP-10	**Information System Recovery and Reconstitution**
		CP-12	**Safe Mode**
FPT_RCV.4	**Trusted Recovery** Function Recovery	SI-6	**Security Function Verification**
		SI-10(3)	**Information Input Validation** Predictable Behavior
		SC-24	**Fail in Known State**
FPT_RPL.1	**Replay Detection** Replay Detection	IA-2(8)	**Identification and Authentication (Organizational Users)** Network Access To Privileged Accounts - Replay Resistant
		IA-2(9)	**Identification and Authentication (Organizational Users)** Network Access To Non-Privileged Accounts - Replay Resistant
		SC-23	**Session Authenticity**
		SI-3(9)	**Malicious Code Protection** Authenticate Remote Commands
FPT_SSP.1	**State Synchrony Protocol** Simple Trusted Acknowledgement	No Mapping.	
FPT_SSP.2	**State Synchrony Protocol** Mutual Trusted Acknowledgement	No Mapping.	
FPT_STM.1	**Time Stamps** Reliable Time Stamps	AU-8	**Time Stamps**
FPT_TDC.1	**Inter-TSF TSF Data Consistency** Inter-TSF Basic Data Consistency	AC-16(7)	**Security Attributes** | Consistent Attribute Interpretation
		AC-16(8)	**Security Attributes** Association Techniques/Technologies
FPT_TEE.1	**Testing of External Entities** Testing of External Entities	SI-6	**Security Functionality Verification**
FPT_TRC.1	**Internal TOE TSF Data Replication Consistency** Internal TSF Consistency	SI-7	**Software, Firmware, and Information Integrity**
FPT_TST.1	**TSF Self-Test** TSF Testing	SI-6	**Security Functionality Verification**
		SI-7	**Software, Firmware, and Information Integrity**
FRU_FLT.1	**Fault Tolerance** Degraded Fault Tolerance	AU-15	**Alternate Audit Capability**
		CP-11	**Alternate Communications Protocols**
		SC-24	**Fail in Known State**
		SI-13	**Predictable Failure Prevention**
		SI-13(1)	**Predictable Failure Prevention** Transferring Component Responsibilities

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
		SI-13(2)	**Predictable Failure Prevention** Time Limit on Process Execution Without Supervision
		SI-13(3)	**Predictable Failure Prevention** Manual Transfer Between Components
		SI-13(4)	**Predictable Failure Prevention** Standby Component Installation/Notification
		SI-13(5)	**Predictable Failure Prevention** Failover Capability
FRU_FLT.2	**Fault Tolerance** Limited Fault Tolerance	AU-15	**Alternate Audit Capability**
		CP-11	**Alternate Communications Protocols**
		SC-24	**Fail in Known State**
		SI-13	**Predictable Failure Prevention**
		SI-13(1)	**Predictable Failure Prevention** Transferring Component Responsibilities
		SI-13(2)	**Predictable Failure Prevention** Time Limit on Process Execution Without Supervision
		SI-13(3)	**Predictable Failure Prevention** Manual Transfer Between Components
		SI-13(4)	**Predictable Failure Prevention** Standby Component Installation/Notification
		SI-13(5)	**Predictable Failure Prevention** Failover Capability
FRU_PRS.1	**Priority of Service** Limited Priority of Service	SC-6	**Resource Availability**
FRU_PRS.2	**Priority of Service** Full Priority of Service	SC-6	**Resource Availability**
FRU_RSA.1	**Resource Allocation** Maximum Quotas	SC-6	**Resource Availability**
FRU_RSA.2	**Resource Allocation** Minimum and Maximum Quotas	SC-6	**Resource Availability**
FTA_LSA.1	**Limitation on Scope of Selectable Attributes** Limitation on Scope of Selectable Attributes	AC-2(6)	**Account Management** Dynamic Privilege Management
		AC-2(11)	**Account Management** Usage Conditions
FTA_MCS.1	**Limitation on Multiple Concurrent Sessions** Basic Limitation on Multiple Concurrent Sessions	AC-10	**Concurrent Session Control**
FTA_MCS.2	**Limitation on Multiple Concurrent Sessions** Per-User Limitation on Multiple Concurrent Sessions	AC-10	**Concurrent Session Control**
FTA_SSL.1	**Session Locking and Termination** TSF-Initiated Session Locking	AC-11	**Session Lock**
		AC-11(1)	**Session Lock** Pattern-Hiding Displays
FTA_SSL.2	**Session Locking and Termination** User-Initiated Locking	AC-11	**Session Lock**
		AC-11(1)	**Session Lock** Pattern-Hiding Displays

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
FTA_SSL.3	**Session Locking and Termination** TSF-Initiated Termination	AC-12	**Session Termination**
		SC-10	**Network Disconnect**
FTA_SSL.4	**Session Locking and Termination** User-Initiated Termination	AC-12(1)	**Session Termination** User-Initiated Logouts / Message Displays
FTA_TAB.1	**TOE Access Banners** Default TOE Access Banners	AC-8	**System Use Notification**
FTA_TAH.1	**TOE Access History** TOE Access History	AC-9	**Previous Login (Access) Notification**
		AC-9(1)	**Previous Login (Access) Notification** Unsuccessful Logons
FTA_TSE.1	**TOE Session Establishment** TOE Session Establishment	AC-2(11)	**Account Management** Usage Conditions
FTP_ITC.1	**Inter-TSF Trusted Channel** Inter-TSF Trusted Channel	IA-3(1)	**Device Identification and Authentication** Cryptographic Bidirectional Authentication
		SC-8	**Transmission Confidentiality and Integrity**
		SC-8(1)	**Transmission Confidentiality and Integrity** Cryptographic or Alternate Physical Protection
FTP_TRP.1	**Trusted Path** Trusted Path	SC-11	**Trusted Path**
	Assurance Requirements		
ASE_INT.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**ST Introduction** ST Introduction	SA-4	**Acquisition Process**
ASE_CCL.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Conformance Claims** Conformance Claims	PL-2	**System Security Plan**
		SA-4(7)	**Acquisition Process** NIAP-Approved Protection Profiles
ASE_SPD.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Security Problem Definition** Security Problem Definition	PL-2	**System Security Plan**
		SA-4	**Acquisition Process**
ASE_OBJ.1 EAL1	**Security Objectives** Security Objectives for the Operational Environment	PL-2	**System Security Plan**
		SA-4	**Acquisition Process**
ASE_OBJ.2 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Security Objectives** Security Objectives	PL-2	**System Security Plan**
		SA-4	**Acquisition Process**

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
ASE_ECD.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Extended Components Definition** Extended Components Definition	No Mapping.	
ASE_REQ.1 EAL1	**Security Requirements** Stated Security Requirements	PL-2	**System Security Plan**
		SA-4	**Acquisition Process**
ASE_REQ.2 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Security Requirements** Derived Security Requirements	PL-2	**System Security Plan**
		SA-4	**Acquisition Process**
ASE_TSS.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**TOE Summary Specification** TOE Summary Specification	PL-2	**System Security Plan**
		SA-4(1)	**Acquisition Process** Functional Properties of Security Controls
ASE_TSS.2	**TOE Summary Specification** TOE Summary Specification with Architectural Design Summary	PL-2	**System Security Plan**
		SA-4(1)	**Acquisition Process** Functional Properties of Security Controls
		SA-4(2)	**Acquisition Process** Design / Implementation Information For Security Controls
		SA-17	**Developer Security Architecture and Design**
ADV_ARC.1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Security Architecture** Security Architecture Description	AC-25	**Reference Monitor**
		SA-17	**Developer Security Architecture and Design**
		SA-18	**Tamper Resistance and Detection**
		SC-3	**Security Function Isolation**
		SC-3(1)	**Security Function Isolation** Hardware Separation
		SC-3(2)	**Security Function Isolation** Minimize Nonsecurity Functionality
		SC-41	**Process Isolation**
ADV_FSP.1 EAL1	**Functional Specification** Basic Functional Specification	SA-4(1)	**Acquisition Process** Functional Properties of Security Controls
		SA-4(2)	**Acquisition Process** Design / Implementation Information for Security Controls
ADV_FSP.2 EAL2	**Functional Specification** Security-Enforcing Functional Specification	SA-4(1)	**Acquisition Process** Functional Properties of Security Controls
		SA-4(2)	**Acquisition Process** Design / Implementation Information for Security Controls

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
		SA-17(4)	**Developer Security Architecture and Design** Informal Correspondence
ADV_FSP.3 EAL3	**Functional Specification** Functional Specification With Complete Summary	SA-4(1)	**Acquisition Process** Functional Properties of Security Controls
		SA-4(2)	**Acquisition Process** Design / Implementation Information for Security Controls
		SA-17(4)	**Developer Security Architecture and Design** Informal Correspondence
ADV_FSP.4 EAL4	**Functional Specification** Complete Functional Specification	SA-4(1)	**Acquisition Process** Functional Properties of Security Controls
		SA-4(2)	**Acquisition Process** Design / Implementation Information for Security Controls
		SA-17(4)	**Developer Security Architecture and Design** Informal Correspondence
ADV_FSP.5 EAL5 EAL6	**Functional Specification** Complete Semi-Formal Functional Specification with Additional Error Information	SA-4(1)	**Acquisition Process** Functional Properties of Security Controls
		SA-4(2)	**Acquisition Process** Design / Implementation Information for Security Controls
		SA-17(4)	**Developer Security Architecture and Design** Informal Correspondence
ADV_FSP.6 EAL7	**Functional Specification** Complete Semi-Formal Functional Specification with Additional Formal Specification	SA-4(1)	**Acquisition Process** Functional Properties of Security Controls
		SA-4(2)	**Acquisition Process** Design / Implementation Information for Security Controls
		SA-17(3)	**Developer Security Architecture and Design** Formal Correspondence
		SA-17(4)	**Developer Security Architecture and Design** Informal Correspondence
ADV_IMP.1 EAL4 EAL5	**Implementation Representation** Implementation Representation of the TSF	SA-4(2)	**Acquisition Process** Design / Implementation Information for Security Controls
ADV_IMP.2 EAL6 EAL7	**Implementation Representation** Complete Mapping of the Implementation Representation of the TSF	SA-4(2)	**Acquisition Process** Design / Implementation Information for Security Controls
		SA-17(3)	**Developer Security Architecture and Design** Formal Correspondence
ADV_INT.1	**TSF Internals** Well-Structured Subset of TSF Internals	SA-8	**Security Engineering Principles**
		SC-3(3)	**Security Function Isolation** Minimize Nonsecurity Functionality
		SC-3(4)	**Security Function Isolation** Module Coupling and Cohesiveness
		SC-3(5)	**Security Function Isolation** Layered Structures

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
ADV_INT.2 EAL5	**TSF Internals** Well-Structured Internals	SA-8	**Security Engineering Principles**
		SC-3(3)	**Security Function Isolation** Minimize Nonsecurity Functionality
		SC-3(4)	**Security Function Isolation** Module Coupling and Cohesiveness
		SC-3(5)	**Security Function Isolation** Layered Structures
ADV_INT.3 EAL6 EAL7	**TSF Internals** Minimally Complex Internals	SA-8	**Security Engineering Principles**
		SA-17(5)	**Developer Security Architecture and Design** Conceptually Simple Design
		SC-3(3)	**Security Function Isolation** Minimize Nonsecurity Functionality
		SC-3(4)	**Security Function Isolation** Module Coupling and Cohesiveness
		SC-3(5)	**Security Function Isolation** Layered Structures
		AC-25	**Reference Monitor**
ADV_SPM.1 EAL6 EAL7	**Security Policy Modeling** Formal TOE Security Policy Model	SA-17(1)	**Developer Security Architecture and Design** Formal Policy Model
		SA-17(3)	**Developer Security Architecture and Design** Formal Correspondence
ADV_TDS.1 EAL2	**TOE Design** Basic Design	SA-4(2)	**Acquisition Process** Design / Implementation Information for Security Controls
		SA-17	**Developer Security Architecture and Design**
ADV_TDS.2 EAL3	**TOE Design** Architectural Design	SA-4(2)	**Acquisition Process** Design / Implementation Information for Security Controls
		SA-17	**Developer Security Architecture and Design**
ADV_TDS.3 EAL4	**TOE Design** Basic Modular Design	SA-4(2)	**Acquisition Process** Design / Implementation Information for Security Controls
		SA-17	**Developer Security Architecture and Design**
ADV_TDS.4 EAL5	**TOE Design** Semiformal Modular Design	SA-4(2)	**Acquisition Process** Design / Implementation Information for Security Controls
		SA-17	**Developer Security Architecture and Design**
		SA-17(2)	**Developer Security Architecture and Design** Security Relevant Components
		SA-17(4)	**Developer Security Architecture and Design** Informal Correspondence

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
ADV_TDS.5 EAL6	**TOE Design** Complete Semiformal Modular Design	SA-4(2)	**Acquisition Process** Design / Implementation Information for Security Controls
		SA-17	**Developer Security Architecture and Design**
		SA-17(2)	**Developer Security Architecture and Design** Security Relevant Components
		SA-17(4)	**Developer Security Architecture and Design** Informal Correspondence
ADV_TDS.6 EAL7	**TOE Design** Complete Semiformal Modular Design with Formal High-Level Design Presentation	SA-4(2)	**Acquisition Process** Design / Implementation Information for Security Controls
		SA-17	**Developer Security Architecture and Design**
		SA-17(2)	**Developer Security Architecture and Design** Security Relevant Components
		SA-17(3)	**Developer Security Architecture and Design** Formal Correspondence
		SA-17(4)	**Developer Security Architecture and Design** Informal Correspondence
AGD_OPE.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Operational User Guidance** Operational User Guidance	SA-5	**Information System Documentation**
AGD_PRE.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Preparative Procedures** Preparative Procedures	SA-5	**Information System Documentation**
ALC_CMC.1 EAL1	**CM Capabilities** Labeling of the TOE	CM-9	**Configuration Management Plan**
		SA-10	**Developer Configuration Management**
ALC_CMC.2 EAL2	**CM Capabilities** Use of a CM System	CM-9	**Configuration Management Plan**
		SA-10	**Developer Configuration Management**
ALC_CMC.3 EAL3	**CM Capabilities** Authorization Controls	CM-3	**Configuration Change Control**
		CM-9	**Configuration Management Plan**
		SA-10	**Developer Configuration Management**
ALC_CMC.4 EAL4 EAL5	**CM Capabilities** Production Support, Acceptance Procedures, and Automation	CM-3	**Configuration Change Control**
		CM-3(1)	**Configuration Change Control** Automated Document / Notification / Prohibition of Changes
		CM-3(3)	**Configuration Change Control** Automated Change Implementation
		CM-9	**Configuration Management Plan**

ISO/IEC 15408 REQUIREMENTS		**NIST SP 800-53 CONTROLS**	
		SA-10	**Developer Configuration Management**
ALC_CMC.5 EAL6 EAL7	**CM Capabilities** Advanced Support	CM-3	**Configuration Change Control**
		CM-3(1)	**Configuration Change Control** Automated Document / Notification / Prohibition of Changes
		CM-3(2)	**Configuration Change Control** Test / Validate / Document Changes
		CM-3(3)	**Configuration Change Control** Automated mechanisms to field and deploy
		CM-9	**Configuration Management Plan**
		SA-10	**Developer Configuration Management**
ALC_CMS.1 EAL1	**CM Scope** TOE CM Coverage	CM-9	**Configuration Management Plan**
		SA-10	**Developer Configuration Management**
ALC_CMS.2 EAL2	**CM Scope** Parts of the TOE CM Coverage	CM-9	**Configuration Management Plan**
		SA-10	**Developer Configuration Management**
ALC_CMS.3 EAL3	**CM Scope** Implementation Representation CM Coverage	CM-9	**Configuration Management Plan**
		SA-10	**Developer Configuration Management**
ALC_CMS.4 EAL4	**CM Scope** Problem Tracking CM Coverage	CM-9	**Configuration Management Plan**
		SA-10	**Developer Configuration Management**
ALC_CMS.5 EAL5 EAL6 EAL7	**CM Scope** Development Tools CM Coverage	CM-9	**Configuration Management Plan**
		SA-10	**Developer Configuration Management**
ALC_DEL.1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Delivery** Delivery Procedures	MP-5	**Media Transport**
		SA-10(1)	**Developer Configuration Management** Software / Firmware Integrity Verification
		SA-10(6)	**Developer Configuration Management** Trusted Distribution
		SA-18	**Tamper Resistance and Detection**
		SA-19	**Component Authenticity**
ALC_DVS.1 EAL3 EAL4 EAL5	**Development Security** Identification of Security Measures	SA-1	**System and Services Acquisition Policy and Procedures**
		SA-3	**System Development Lifecycle**
		SA-12	**Supply Chain Protection**
ALC_DVS.2 EAL6 EAL7	**Development Security** Sufficiency of Security Measures	CM-5	**Access Restrictions for Change**
		SA-3	**System Development Lifecycle**
		SA-12	**Supply Chain Protection**
ALC_FLR.1	**Flaw Remediation** Basic Flaw Remediation	SA-10	**Developer Configuration Management**
		SA-11	**Developer Security Testing / Evaluation**
		SI-2	**Flaw Remediation**
ALC_FLR.2	**Flaw Remediation** Flaw Reporting Procedures	SA-10	**Developer Configuration Management**
		SA-11	**Developer Security Testing / Evaluation**
		SI-2	**Flaw Remediation**
ALC_FLR.3	**Flaw Remediation** Systematic Flaw Remediation	SA-10	**Developer Configuration Management**
		SA-11	**Developer Security Testing / Evaluation**
		SI-2	**Flaw Remediation**

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
ALC_LCD.1 EAL3 EAL4 EAL5 EAL6	**Life-Cycle Definition** Developer Defined Life-Cycle Model	SA-3	**System Development Life Cycle**
		SA-15	**Development Process, Standards, and Tools**
ALC_LCD.2 EAL7	**Life-Cycle Definition** Measurable Life-Cycle Model	SA-3	**System Development Life Cycle**
		SA-15	**Development Process, Standards, and Tools**
ALC_TAT.1 EAL4	**Tools and Techniques** Well-Defined Development Tools	SA-15	**Development Process, Standards, and Tools**
ALC_TAT.2 EAL5	**Tools and Techniques** Compliance with Implementation Standards	SA-15	**Development Process, Standards, and Tools**
ALC_TAT.3 EAL6 EAL7	**Tools and Techniques** Compliance with Implementation Standards – All Parts	SA-15	**Development Process, Standards, and Tools**
ATE_COV.1 EAL2	**Coverage** Evidence of Coverage	SA-11	**Developer Security Testing and Evaluation**
		SA-11(7)	**Developer Security Testing and Evaluation** *Verify Scope of Testing / Evaluation*
ATE_COV.2 EAL3 EAL4 EAL5	**Coverage** Analysis of Coverage	SA-11	**Developer Security Testing and Evaluation**
		SA-11(7)	**Developer Security Testing and Evaluation** *Verify Scope of Testing / Evaluation*
ATE_COV.3 EAL6 EAL7	**Coverage** Rigorous Analysis of Coverage	SA-11	**Developer Security Testing and Evaluation**
		SA-11(7)	**Developer Security Testing and Evaluation** *Verify Scope of Testing / Evaluation*
ATE_DPT.1 EAL3	**Depth** Testing: Basic Design	SA-11	**Developer Security Testing and Evaluation**
		SA-11(7)	**Developer Security Testing and Evaluation** *Verify Scope of Testing / Evaluation*
ATE_DPT.2 EAL4	**Depth** Testing: Security Enforcing Modules	SA-11	**Developer Security Testing and Evaluation**
		SA-11(7)	**Developer Security Testing and Evaluation** *Verify Scope of Testing / Evaluation*
ATE_DPT.3 EAL5 EAL6	**Depth** Testing: Modular Design	SA-11	**Developer Security Testing and Evaluation**
		SA-11(7)	**Developer Security Testing and Evaluation** *Verify Scope of Testing / Evaluation*
ATE_DPT.4 EAL7	**Depth** Testing: Implementation Representation	SA-11	**Developer Security Testing and Evaluation**
		SA-11(7)	**Developer Security Testing and Evaluation** *Verify Scope of Testing / Evaluation*
ATE_FUN.1 EAL2 EAL3 EAL4 EAL5	**Functional Tests** Functional Testing	SA-11	**Developer Security Testing and Evaluation**
ATE_FUN.2 EAL6 EAL7	**Functional Tests** Ordered Functional Testing	SA-11	**Developer Security Testing and Evaluation**
ATE_IND.1 EAL1	**Independent Testing** Independent Testing – Conformance	CA-2	**Security Assessments**
		CA-2(1)	**Security Assessments** *Independent Assessors*
		SA-11(3)	**Developer Security Testing and Evaluation** *Independent Verification of Assessment Plans / Evidence*

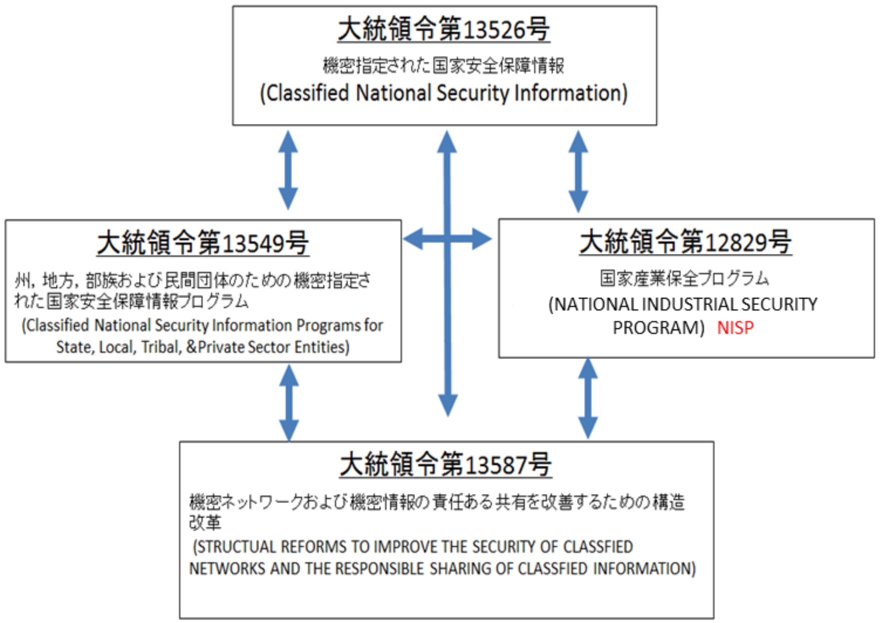
ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
ATE_IND.2 EAL2 EAL3 EAL4 EAL5 EAL6	**Independent Testing** Independent Testing – Sample	CA-2	**Security Assessments**
		CA-2(1)	**Security Assessments** *Independent Assessors*
		SA-11(3)	**Developer Security Testing and Evaluation** *Independent Verification of Assessment Plans / Evidence*
ATE_IND.3 EAL7	**Independent Testing** Independent Testing – Complete	CA-2	**Security Assessments**
		CA-2(1)	**Security Assessments** *Independent Assessors*
		SA-11(3)	**Developer Security Testing and Evaluation** *Independent Verification of Assessment Plans / Evidence*
AVA_VAN.1 EAL1	**Vulnerability Analysis** Vulnerability Survey	CA-2(2)	**Security Assessments** *Specialized Assessments*
		CA-8	**Penetration Testing**
		RA-3	**Risk Assessment**
		SA-11(2)	**Developer Security Testing and Evaluation** *Threat And Vulnerability Analyses / Flaw Remediation*
		SA-11(5)	**Developer Security Testing and Evaluation** *Penetration Testing*
AVA_VAN.2 EAL2 EAL3	**Vulnerability Analysis** Vulnerability Analysis	CA-2(2)	**Security Assessments** *Specialized Assessments*
		CA-8	**Penetration Testing**
		RA-3	**Risk Assessment**
		SA-11(2)	**Developer Security Testing and Evaluation** *Threat And Vulnerability Analyses / Flaw Remediation*
		SA-11(5)	**Developer Security Testing and Evaluation** *Penetration Testing*
AVA_VAN.3 EAL4	**Vulnerability Analysis** Focused Vulnerability Analysis	CA-2(2)	**Security Assessments** *Specialized Assessments*
		CA-8	**Penetration Testing**
		RA-3	**Risk Assessment**
		SA-11(2)	**Developer Security Testing and Evaluation** *Threat And Vulnerability Analyses / Flaw Remediation*
		SA-11(5)	**Developer Security Testing and Evaluation** *Penetration Testing*
AVA_VAN.4 EAL5	**Vulnerability Analysis** Methodical Vulnerability Analysis	CA-2(2)	**Security Assessments** *Types of Assessments*
		CA-8	**Penetration Testing**
		RA-3	**Risk Assessment**
		SA-11(2)	**Developer Security Testing and Evaluation** *Threat And Vulnerability Analyses / Flaw Remediation*
		SA-11(5)	**Developer Security Testing and Evaluation** *Penetration Testing*
AVA_VAN.5 EAL6 EAL7	**Vulnerability Analysis** Advanced Methodical Vulnerability Analysis	CA-2(2)	**Security Assessments** *Types of Assessments*
		CA-8	**Penetration Testing**
		RA-3	**Risk Assessment**

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
		SA-11(2)	**Developer Security Testing and Evaluation** *Threat And Vulnerability Analyses / Flaw Remediation*
		SA-11(5)	**Developer Security Testing and Evaluation** *Penetration Testing*
ACO_COR.1	**Composition Rationale** Composition Rationale	SA-17	**Developer Security Architecture and Design**
ACO_DEV.1	**Development Evidence** Functional Description	SA-17	**Developer Security Architecture and Design**
ACO_DEV.2	**Development Evidence** Basic Evidence of Design	SA-17	**Developer Security Architecture and Design**
ACO_DEV.3	**Development Evidence** Detailed Evidence of Design	SA-17	**Developer Security Architecture and Design**
ACO_REL.1	**Reliance on Dependent Component** Basic Reliance Information	SA-17	**Developer Security Architecture and Design**
ACO_REL.2	**Reliance on Dependent Component** Reliance Information	SA-17	**Developer Security Architecture and Design**
ACO_CTT.1	**Composed TOE Testing** Interface Testing	SA-11	**Developer Security Testing and Evaluation**
ACO_CTT.2	**Composed TOE Testing** Rigorous Interface Testing	SA-11	**Developer Security Testing and Evaluation**
ACO_VUL.1	**Composition Vulnerability Analysis** Composition Vulnerability Review	CA-2	**Security Assessments**
		CA-8	**Penetration Testing**
		RA-3	**Risk Assessment**
		SA-11	**Developer Security Testing and Evaluation**
ACO_VUL.2	**Composition Vulnerability Analysis** Composition Vulnerability Analysis	CA-2	**Security Assessments**
		CA-8	**Penetration Testing**
		RA-3	**Risk Assessment**
		SA-11	**Developer Security Testing and Evaluation**
ACO_VUL.3	**Composition Vulnerability Analysis** Enhanced-Basic Composition Vulnerability Review	CA-2	**Security Assessments**
		CA-8	**Penetration Testing**
		RA-3	**Risk Assessment**
		SA-11	**Developer Security Testing and Evaluation**

NISPOM (National Industrial Security Program Operation Manual)

- 米国の国家産業保全プログラム（NISP）の運用マニュアル(DoD 5220.22-M)。
- NISPは機密情報（Classified information）を保護するための連邦政府と民間企業との間のパートナーシップである。
- NISPOMでは米国政府の請負業者の個人や施設のクリアランスを行い決定を下すためのガイドラインと範囲を設定している。
- 換言すると、NISP / NISPOM は認可施設においてセキュリティクリアランスを持つ個人が機密情報のセキュリティを扱うという構成である。
- NISPOMは1995年の初版以来、数回の改定が行われている。

NISPと各大統領令の関係

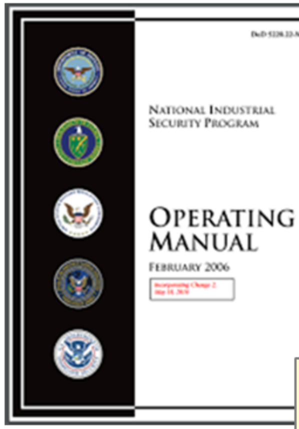


大統領令第13526号
機密指定された国家安全保障情報
(Classified National Security Information)

大統領令第13549号
州, 地方, 部族および民間団体のための機密指定された国家安全保障情報プログラム
(Classified National Security Information Programs for State, Local, Tribal, &Private Sector Entities)

大統領令第12829号
国家産業保全プログラム
(NATIONAL INDUSTRIAL SECURITY PROGRAM) NISP

大統領令第13587号
機密ネットワークおよび機密情報の責任ある共有を改善するための構造改革
(STRUCTUAL REFORMS TO IMPROVE THE SECURITY OF CLASSFIED NETWORKS AND THE RESPONSIBLE SHARING OF CLASSFIED INFORMATION)



NISPOM構成

1. 総則及び一般的要件
2. セキュリティクリアランス
3. セキュリティトレーニング
4. 秘密区分と標記
5. 秘密指定情報の保護対策
6. 立ち入り及び会合
7. 下請契約
8. 情報システム・セキュリティ
9. 特別要件
10. 国際的セキュリティ要件
11. 雑則

NISPOM　各章の概要

Chapter 1.　総則及び一般的要件
NISPOMの法的位置付けや企業等の組織要件、通報の要請について解説している。

序節：NIPOMの位置づけは、NISPのオペレーションマニュアルであり、NISPは大統領令第13526号と原子力法に基づいている。監督権限は各連邦省庁または機関（「管轄保全局（CSA）」等）に属する。
2節：請負業者は機密情報が義務付けられており、施設保全適格性確認（FCL）の一環として施設保全担当者（FSO）を任命しなければならない。
3節：請負業者はFCLやPCLに影響を及ぼす出来事や、機密情報の適切な保護に影響を及ぼす出来事があった場合にFSO、FBIまたは連邦政府に対して報告が求められる。報告の方法も規定されている。

Chapter 2. セキュリティクリアランス
施設クリアランス、人的クリアランス、FOCI（外国による所有、管理または影響）について規定している。

1節：施設クリアランス（FCL）：施設が秘密情報のアクセスまたは秘密関連契約の締結について適格であるという行政が決定した場合にFCLが交付される。申請のプロセスや要求事項について規定されている。またFCLがクリアされるためには、いくつかの主要な経営幹部の人的クリアランスもクリアする必要がある。
2節：人的クリアランス（PCL）：FSOはアクセスが不可欠と認めた場合に従業員に秘密保持を指示し、人的なクリアランスを実施しなければならない。
3節：FOCI（外国による所有、管理または影響）：外国企業の影響下にあると判断される場合はアクセス制御の対象となる。FOCIを無効化するためには会社の理事会あるいは特殊な協定を結び、その中でいくつかの組織・人事的要求がなされる。

Chapter 3. セキュリティ・トレーニング
PCL保有者への研修についての規定している。

1節：請負業者は、PCLを保有する全ての者にセキュリティ・トレーニングを行わなければならず、その資料や派遣業者への対応が規定されている。また、アクセス許可に先立ちブリーフィングを行わなければならないこと、少なくとも年1回の継続的実施も規定されている。

Chapter 4.　機密区分と標記
機密の区分と標記（マーキング）要件について解説している。

1節：機密はTOP SECRET（TS），SECRET（S），CONFIDENTIAL（C）に区分されている。時間の経過やその他により、秘密区分の指定は解除または格下げになる場合がある。
2節：保護の程度を警告・通知するために、全ての秘密情報に物理的な標記（秘密区分のレベル、秘密情報が含まれている箇所、保護の期間等）を行うこととしている。標記方法は細部にわたり規定されており、例えば派生機密（原機密を織り込んだり、言い換えたりしたもの）についても、その範囲を明確に説明し、請負業者が自身の秘密区分マニュアルを作成して適切に指定しなくてはならない。

Chapter 5. 機密指定情報の保護対策

管理に関する主文として、保管中の情報の物理的保護に係る要件について記載。一般的要求事項、管理と責任追跡性、保管と保管装置、伝送、開示、複製、処分と保有、構造の要求、不正侵入検知システムについて詳細な具体的要件が規定されている。

1節：受託業者は、機密情報を保護する責任があり、個人は個人に預けられた機密情報を保護する責任がある。
2節：受託業者は、機密情報の情報管理システムについて、その管理と説明責任を負っている。
3節：機密譲歩の保管に関する統一的な物理的保護要件が規定されている。例えば、保管容器や錠前等はGSA（共通役務庁）が承認したものを用いること、機密の区分により保護対策のレベルが分けらること、制限区域や閉鎖区域の設置方法、保護容器、キャビネット、金庫室、錠前等の保護や管理方法、アクセス制限システムの要件等が細部にわたり規定されている。
4節：機密情報を施設外に送達する場合の、秘密区分に応じた承認プロセス、海外の区分、梱包・輸送方法等が詳細に規定されている。
5節：機密情報の開示は、確実に承認した人物だけを対象に行うこととされており、対象となる従業員、下請け会社、親子会社、MFO、DoD、連邦政府、外国人等に応じた方法が規定されている。
6節：機密情報の複製に関して、制限、方法、記録について規定されている。
7節：不要となった機密情報への適切な処分の方法について、返却または破壊の具体的な方法が規定されている。
8節：閉鎖区域および金庫室の構造物に関して、壁、窓、扉、施錠装置、天井、扉、骨組ユニット、その他開口部に至るまで詳細に具体的要件が規定されている。
9節：特にTOP SECRETとSECRETに対して追加の保護策が要求された場合に、不正侵入検知システム（IDS）の最低限の規格が規定されている。

Chapter 6.　立ち入り及び会合

機密を扱う施設が訪問を受ける場合の守るべき規則、会議における分類された情報の開示等を規定している。

1節：受託業者や連邦政府の施設へ訪問する場合の要求事項が規定されている。訪問回数の制限、訪問者のPCL確認等。
2節：機密情報が開示される会議等の開催に関する要件が規定されている。開催申請、会議場所、情報開示の申請等。

Chapter 7.　下請契約

機密情報を下請事業者に開示する際の元請受託事業者の要件と責任について規定している。

1節：下請事業者に対して機密情報を開示する場合、契約前の保全適格性やセキュリティ対策の確認、ガイダンス等、機密区分指定仕様書への文書規定、履行後の保持継続が規定されている。

Chapter 8.　情報システム・セキュリティ

情報システム関する義務及び責任、評価および認可、セキュリティ管理策について規定している。初版以降、最も改変の多い章。

1節：機密情報の取込、作成、保存、処理または配布の際に適切に管理されるよう、受託業者はCSAガイダンスに基づいたISセキュリティプログラムによりセキュリティ計画（情報システム責任者、同管理者、同ユーザーの規定等）を策定しなければならない。
2節：セキュリティ計画を評価し認可するのはCSAから指名された権限を持った職員が行うが、受託業者のセキュリティ管理は共同で取り組むものとしている。
3節：セキュリティ管理に関する具体的な保護要求事項が詳細に規定されている。データ消去、ハード・ソフトウェアの検査、識別・認証管理、保守、媒体への標記、等についてベースラインを設定しリスクコントロールを図り、技術的人的物理的環境的保護を実施し緊急時対応・構成管理を行い運用管理を行う。
また、モバイルシステムについては特別の手順書を作成する必要がある。（情報システムインシデントレスポンスを含む）

Chapter 9.　特別要件

特別に指定された情報に関する特別要件について規定している。

核関連の制限データ（RD）、旧制限データ（FRD）、DOE指令に基づき機密指定された外国原子力情報（TFNI）（第1節; 詳細は付属書D）、国防総省重要核兵器設計情報（CNWDI）（第2節）、諜報情報（第3節）、通信秘密保全（COMSEC）（第4節）についての特別要件事項を規定する。

Chapter 10.　国際的セキュリティ要件

国家間プログラムにおける機密情報管理に係る方針と手続きについて規定している。

1節：合衆国内外を問わず、物品、役務および関連技術データを外国人に譲渡すること、又はこれらの資料もしくは情報を合衆国の法的管轄権外の目的地に移動することは、輸出に該当する。物品、またはデータの特性にもよるが、ほとんどの輸出は武器輸出管理法（AECA）、輸出管理法（EAA）、原子力法（AEA）によって管理される。

1節を踏まえ、外国権益に対する米国情報の開示（第2節）、外国政府情報（第3節）、国際移転（第4節）、外国からの訪問及び外国人の管理（例えば外国人のアクセスがある場合には技術保全計画作成する必要があるなど）（第5節）、請負業者の海外活動（第6節）、NATOの情報セキュリティ要件（第7節）、ライセンスあるいは授権書がない場合の豪州および英国への防衛物品の移転（第8節）について規程する。

Chapter 11.　雑則

テンペスト（TEMPEST）、国防技術情報センター（DTIC）、独自の研究開発について規定している。

1節：テンペスト（TEMPEST）要件の適用と費用について規程する。テンペストとは、不正侵入する電磁放射に関する調査および研究を意味する非機密指定の省略名である。不正に侵入する電磁放射は、意図せざる諜報伝達信号で、万が一傍受・分析された場合には、何らかの情報処理機器を通じて送信、受信、操作、または処理する際に、機密情報が開示される。テンペスト要件が適用される場合、政府の契約機関（GCA）は、必要とされる対策について書面で確認する。

2節：国防技術情報センター（DTIC）は、国防総省のRDT&Eおよび調査プログラムを支援するための科学技術情報を取得、保管、検索、普及の役割を担う。第10章2節では、実施中/ 計画中のRDT&Eについて説明した科学技術情報へのアクセスに関して、DTICが個人または組織を支援する際の規程を記す。

3節：契約事業者のIR＆D（独自の研究開発）活動に組み込まれた機密情報を保護するための、特別の手続および要求事項を規定する（たとえば、契約事業者のIR&D成果の情報は派生的な機密区分の指定を必要とする。独自の研究開発等に利用する場合には独自のセキュリティマニュアルを作成する必要がある等）。