		情報セキュリティ基準に関するよくあるご質問	回答
A.		全般に関するご質問	
	A-01	情報セキュリティ基準とは何ですか？	防衛省が指定する保護すべき情報を契約企業が取り扱う際に、防衛省が当該企業に求める保護対策（セキュリティ管理策）の水準を纏めたものです。NIST SP800-171と同等のセキュリティ要求事項となっています。このうち、第９条（保護システムに関する要求）は、要求事項も多岐に亘ることからシステム面の管理策として別冊（システムセキュリティ実施要領）にまとめています。
	A-02	どのような場合に情報セキュリティ基準が適用されるのですか？	令和５年４月１日以降の装備品等及び役務の調達にかかる防衛省との契約のうち、保護すべき情報の取扱いが含まれるすべての契約が適用の対象です。これらの契約の特約条項（別紙）として、A-01の情報セキュリティ基準を充たす管理策を講じることを契約上の要件としています。
	A-03	下請負企業にも適用されますか？	特約条項で下請負企業にも適用することを規定しています。また、孫請け以降の企業がいる場合にも適用されます。
	A-04	適用対象外となるのはどういう場合ですか？	防衛省と外国政府または国際機関、日本政府と外国政府間の情報保護協定等の特別な取り扱いが適用される調達は対象外です。ただし、適用除外の調達においても、保護すべき情報を取り扱う場合は、特約条項に準じた 契約条項等が付されますので、予めご承知おきください。
B.		情報セキュリティ基準及び関連する規則類に関するご質問	
	B-01	情報セキュリティの確保に関連する規則にはどのようなものがありますか？	情報セキュリティ基準等については複数あります。Webサイト（https://www.mod.go.jp/atla/cybersecurity.html）を参照してください。
	B-02	保護すべき情報とは何ですか？	装備品等及び役務の調達に関する情報のうち、防衛省の職員以外の者で当該事務に関与しない職員にみだりに知られることが業務の遂行に支障を与えるおそれのあるとして、防衛省から指定された注意情報等をさします。これらは、防衛省から提供する情報のみならず、契約の過程で企業側で生成される情報も含みます。迷う場合は、防衛省（指定書を作成した部署）にご確認ください。
C.		契約前の準備のご質問	
	C-01	現在防衛省との契約はありませんが将来に向けて情報セキュリティ基準に対応したいと考えています。どうすればいいですか？	契約がなくても新基準対応について事前に相談いただくことは可能です。正式には契約担当官宛の照会となりますが、事前に情報セキュリティ基準相談窓口（industrial-cybersecurity-office@ext.atla.mod.go.jp）にお問い合わせ頂くことで、準備内容の過不足などを予め調整、確認できるため、後続の対応がスムーズです。
D.		事業計画に関するご質問	
	D-01	何のためのドキュメントですか？	令和５年４月１日施行の新情報セキュリティ基準に、適合するための組織的な環境整備に時間を要し、契約時点から新基準適合をすることが困難である企業が、対応が困難であることの合理的な理由と、極力早期に新基準に適合するための適切なスケジュールを示し、防衛省と合意するために提出するドキュメントです。 本ドキュメントで合意した期日までは新基準適合を猶予し、旧基準による契約履行を認める経過措置が適用されます。このため、期日を過ぎて旧基準のまま契約を履行することは認めておりません。やむを得ない事由により適用期間の変更を要する場合は速やかに防衛省に相談してください（D-07参照）
	D-02	どのような場合に作成・提出が必要ですか？	令和５年４月１日以降に、特約付き契約を締結する企業が、即時に新基準対応が困難である場合に作成・提出が必要になります。最初から新基準に適合する組織体制やシステム環境等が整備されている企業は、作成・提出の必要はありません。
	D-03	経過措置の適用期間（期限）はどのように設定しますか？	令和５年４月１日以降で新基準が施行されていること、さらに近年のセキュリティリスクの高まりを踏まえ、できるだけ早期に、新情報セキュリティ基準に適合できるよう計画してください。 規則上は経過措置の廃止される令和10（2028）年３月末までとなりますが、施行されて1年経過の実績からほとんどの防衛関連企業では１，２年の間に切換えを完了する予定でご協力頂いております。
	D-04	提出するのはいつですか。どのくらい時間がかかりますか？	防衛省による確認は最大で２ヶ月程度を見込んでください。契約締結前にもご相談を随時受けつけておりますので、受注にあたっては現実的な事業計画を申請いただくようお願いします。 特に、契約締結後に特段の合理的な理由がないまま承認済みの事業計画を変更したい旨の要請が散見されます。これらの要請は防衛省がやむを得ないと認められる事情がない限りは、原則として計画の変更は認められません（契約違反となります）。こうした事のないよう、内容を十分に検討のうえ、事業計画を提出してください。
	D-05	提出するための「ひな形」はありますか？	Webサイト（https://www.mod.go.jp/atla/cybersecurity.html）の（提出資料）を参照してください。
	D-06	提出先はどこですか？	提出先は、契約担当官です。事前に情報セキュリティ基準相談窓口（industrial-cybersecurity-office@ext.atla.mod.go.jp）で書類内容の確認をしております。特に初めて提出する場合等は、情報セキュリティ基準相談窓口で事前確認をうけてから契約担当官に提出すると、後続の手続きがスムーズに進みます（推奨）
	D-07	既に承認されている事業計画書の内容に変更が生じるかもしれません。どうすればいいですか	変更の見込みが生じた場合は速やかに防衛省に相談してください。極力早期に対応いただきたいセキュリティ対策であることを踏まえ、合理的な理由を説明いただく必要があります。変更理由の合理性について、迷う場合は前広に情報セキュリティ基準相談窓口（industrial-cybersecurity-office@ext.atla.mod.go.jp）にご照会ください。
E.		情報セキュリティ基本方針等に関するご質問	
	E-01	何のためのドキュメントですか？	各社の情報セキュリティのための取り組みを示すものであり、このうち、情報セキュリティ規則で情報セキュリティ基準の要求事項に沿った組織体制や環境による企業統制の方針やルールを整備し、情報セキュリティ実施手順では、同基準の付紙であるシステムセキュリティ実施要領の要求事項に沿って主に保護システムの実装・運用に関する統制の方針やルールを整備します。
	E-02	どのような場合に作成・提出が必要ですか？	保護すべき情報の取扱いが含まれるすべての契約には、作成・提出が必要です。このうち保護システムを使用しない契約については、情報セキュリティ実施手順は必要ありません。
F.		システムセキュリティ実装計画書に関するご質問	
	F-01	何のためのドキュメントですか？	保護すべき情報を取り扱う保護システムが情報セキュリティ基準に適合した十分なセキュリティ実装がされていることを証明するために各企業が作成するドキュメントです。作成した内容は防衛省の確認を受ける必要があります。
	F-02	どのような場合に作成・提出が必要ですか？	保護システムで保護すべき情報（保護すべきデータ）を取り扱う場合は作成が必要です。保護システムがない場合は作成する必要はありません。提出については「ひな形」があるため後述を参照してください。
	F-03	契約ごとに作成する必要はありますか？	契約ごとに作成する必要はありません。システムセキュリティ実装計画書は、保護システムごとに行います。 但し、保護システムの形態変更など大幅に変更した場合は、新規作成が必要です。
	F-04	契約ごとに提出する必要はありますか？	契約ごとに提出は必要です。初回は、契約担当官宛てに装装保第4208号・別記様式第５の書式を使用して提出してください。既に防衛省の承認を受けた後で、保護システムに変更がなくそのまま活用する場合、契約担当官宛てに装装保第4243号・別記様式第５の書式を使用して、その旨を提出してください。
	F-05	提出するのはいつですか、どのくらい時間がかかりますか？	情報セキュリティ基本方針等の作成が完了した後に提出し、当該契約期間における保護システムで保護すべき情報（データ）を取り扱う前迄に防衛省の確認が済んでいる必要があります。提出されたシステムセキュリティ実装計画書に関する防衛省の確認は、提出内容やシステムの構成等にもよりますが、最大２ヶ月程度要しますので、計画的に作成・提出することを推奨します。
	F-06	提出するための決まった「ひな形」はありますか？	各社からの提出内容や防衛省による評価の目線等を平準化するために、「ひな形」があります。 Webサイト（https://www.mod.go.jp/atla/cybersecurity.html）の（提出資料）を参照してください。
	F-07	提出先はどこですか？	提出先は、契約担当官です。事前に情報セキュリティ基準相談窓口（industrial-cybersecurity-office@ext.atla.mod.go.jp）で書類内容の確認をしております。特に初めて提出する場合等は、情報セキュリティ基準相談窓口で事前確認をうけてから契約担当官に提出すると、後続の手続きがスムーズに進みます（推奨）
	F-08	ＤＳＧの環境しかありません。ＤＳＧ窓口への提出や確認は必要ありませんか？	ＤＳＧ窓口への提出や確認の必要はありません。

	F-09	契約期間中に、既に承認されたシステムセキュリティ実装計画書の内容に変更が生じました。再提出は必要ですか？	保護システムの情報セキュリティ実装を変更する場合は、原則として再提出が必要です。ただし、同等の基本構成における端末等の単純増設やパッチ最新化のためのバージョンアップ等のように、セキュリティ設計に影響しないような、既に承認されたセキュリティ運用に伴う軽微な変更であれば防衛省に再提出する必要はありません。他方で、情報セキュリティ基本方針等の規則類やセキュリティ設計の変更を伴うような基本設計の変更は、提出を要する場合があります。迷う場合は情報セキュリティ基準相談窓口（industrial-cybersecurity-office@ext.atla.mod.go.jp）にご照会ください。 なお、提出が必要のない軽微な変更も、防衛省の求めに応じて随時速やかに最新の情報を提出できるよう、更新する必要はあります。企業において適切に管理してください。
	F-10	人事異動によって責任者情報等に変更がありましたが、それ以外の変更はありません。再提出は必要ですか？	各責任者等の人事情報が変更するのみであれば、再提出する必要はありません。なお、実施要領第2.1(2)「（ク）組織体制図」に相当する情報は、企業内で適切に更新してください。また、保護システム利用者かどうかによらず、保護すべき情報を取り扱う「取扱者名簿」の変更と提出（確認依頼）は必要ですのでご留意ください。
G.		その他のご質問	
	G-01	基盤強化法とは何ですか？詳しい内容を教えてください。	情報セキュリティ基準に対応するために必要となる費用面の支出については、防衛省が負担することが可能な場合があります。詳細はWebサイト（https://www.mod.go.jp/atla/hourei_dpb.html）を参照いただき、基盤強化法専用の照会窓口にお問い合わせください。
	G-02	ＤＳＧとは何ですか？詳しい内容を教えてください。	防衛セキュリティゲートウェイ（ＤＳＧ）は防衛省が提供する保護すべき情報を企業と電子的かつセキュアに共有するため通信基盤です。情報セキュリティ基準の一部の管理策については、防衛省が予め実装した状態で環境を提供しているため、企業によるセキュリティ関連の管理負担の軽減が可能です。詳細はWebサイト（https://www.mod.go.jp/atla/dsg.html）を参照いただき、DSG専用の照会窓口にお問い合わせください。
	G-03	ＤＳＧは外部ネットワーク接続として扱う必要がありますか？	ＤＳＧは外部ネットワークとして扱いません。ＤＳＧ担当部署から提供される要領に沿って接続してください。
	G-04	事業計画は、基盤強化法の適用やＤＳＧ導入スケジュールと整合的に計画する必要がありますか？	これから基準に適合するために体制や環境を整備する予定であり、基盤強化法やＤＳＧ導入も希望する場合は、これらの適用や利用可否、申請から導入までのスケジュールと、基準適合の時期が整合的に事業計画に反映されている必要があります。なお、基盤強化法やDSG導入の申請窓口や対応部署は、情報セキュリティ基準の窓口と異なりますので留意が必要です。（基盤強化法は（https://www.mod.go.jp/atla/hourei_dpb.html）、ＤＳＧは（https://www.mod.go.jp/atla/dsg.html）が窓口です。）これらは各窓口と相談しながら余裕をもって申請することで、整合的なスケジュールの設定が可能です。各対応のスケジュールを整合的に計画することが困難である場合は、遠慮なく情報セキュリティ相談窓口（industrial-cybersecurity-office@ext.atla.mod.go.jp）にご相談ください。