NAVFAC
Naval Facilities Engineering Systems Command
NAVFAC Far East

# REMINDER RE:

# FAR 52.204-21- Basic Safeguarding of Covered Contractor Information Systems and the fifteen (15) security controls that all contractors must meet.

# 注意：対象業者の情報システムの基本的防護措置と全業者が満たさなければいけない15の保安措置

Overall Classification: UNCLASSIFIED

# *FAR 52.204-21 – Basic Safeguarding of Covered Contractor Information Systems*

**FAR 52.204-21 – Basic Safeguarding of Covered Contractor Information Systems (対象業者の情報システムの基本的防護措置)**

**– REQUIRES CONTRACTORS TO IMPLEMENT 15 SECURITY CONTROLS TO COVERED CONTRACTOR INFORMATION SYSTEMS (契約業者が対象業者の情報システムに対する15の保安措置を実行する事を必要とする）**

- **Covered Contractor Information Systems –** means an information system that is owned or operated by a contractor that processes, stores, or transmits *Federal contract information*. (対象業者の情報システム – 業者が所有する軍との契約に関する情報を処理、保管および送信する情報システム)

- **Federal Contract Information –** means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (i.e., public web sites) or simple transactional information, such as necessary to process payments. (軍との契約に関する情報 – 契約を実行する為に軍から提供されたり軍用に作られ、尚且つ外部に公開の意図の無い情報。公共のウェブサイト等の軍が一般に公開している情報を除く)

# FAR 52.204-21 – Basic Safeguarding of Covered Contractor Information Systems

− Imposes “basic” requirements – Minimum acceptable standards （「基本的」要求を課す – 許容最低基準)

− Applies to all contracts, except COTS items, including contracts under the Simplified Acquisition Threshold (全ての契約に適用される。市販されている既製品は該当しない)

− Effective June 15, 2016 – A changing area of the law (2016年6月15日施行)

# *The FAR 52.204-21 15 Security Controls Explained in Plain English*

**#1 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). (情報システムアクセスを認可された人に限定、その代理人が行う処理及びデバイスを限定)** People that are not supposed to access your system should be prevented from doing so, allowing only access to authorized individuals with a business need. As a result, this control requires that you have formal processes in place to authorize and document access to your systems and that the access is controlled via an authentication mechanism (i.e. passwords). ( 仕事上システムにアクセスする必要の無い人がアクセスできないようにする。アクセスの許可、システムへのアクセスの記録、またパソワード等の認証機能でアクセス管理する正式な手順を確立する必要がある)

**#2 Limit information system access to the types of transactions and functions that authorized users are permitted to execute. (認可された人が行える処理や機能を限定する)** This control deals with enforcing the concept of “separation of duties”. User’s should only be able to access systems and information required for them to complete their assigned tasks. This can be accomplished with role based access controls. (職務分掌の概念による管理。ユーザーは割り当てられた仕事を行うのに必要なシステムや情報にのみアクセスが可能。ロールベースアクセス制御)

**#3 Verify and control/limit connections to and use of external information systems. (外部情報システムへの接続を確認し管理・制限する)** This control deals with limiting employee use of non-corporate controlled systems such as personal devices, personal cloud storage, or computers at a hotel because you can not verify the security state of those systems and do not have control over the data stored on them. You should not allow contract information on systems you do not control. (個人所有のデバイスやクラウド、ホテルのPC等の会社で管理していないシステムの使用を制限する。これらのシステムのセキュリティー状況が確認不可能な上、それらに保存されたデータの管理ができない。管理できないシステムに契約に関する情報を入れない）

# *The FAR 52.204-21 15 Security Controls Explained in Plain English*

**#4 Control information posted or processed on publicly accessible information systems. (外部からアクセス可能な情報システムでの処理や掲載情報の管理)** This control is pretty straight forward, federal contract information that has not been released to the public by the government should not be stored in any location accessible by the general public. This includes your website, social media, or any other public medium. Policies should be in place to prevent federal contract information from being posted publicly. (軍が公表していない契約に関する情報は外部からアクセスできる場所に保管しない。業者のウェブサイト、ソーシャルメディア、その他公衆媒体を含む。軍との契約に関する情報が公にならないように対策が必要。)

**#5 Identify information system users, processes acting on behalf of users, or devices. (情報システムのユーザー、代理人による処理、及びデバイスを確認する)** In short, accounts used on your systems should be traceable to the person using them. So an account used by John Doe should be named jdoe or John.Doe not Surfer1985. This is especially important if you need to trace back an event to a user when examining audit logs. In some cases shared or service accounts with a non identifying name such as “backupservice” may be necessary, these should be well documented and controlled. (ユーザーがシステムで使用履歴を確認できるようにする。例えば、John Doeという人が使うアカウント名はSurfer1985ではなくjdoeやJohn.Doeのようにする。ユーザー毎の履歴を確認する際に重要になる。ユーザーを特定しないアカウントが必要な場合は、記録に残し管理する)

**#6 Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. (会社の情報システムにアクセスを認める前提条件としてユーザー、処理事項及びデバイスを確認し認可する)** This control seeks to ensure that the subject accessing your system is actually who they claim to be. For example, there may be an account named jdoe but if the password is “1234” then there is no guarantee that John Doe has actually logged in. This is best accomplished by having robust account provisioning and password reset procedures as well as a strong password policy. Two factor authentication (not required for FAR 52.204-21 as of the writing of this guide) is also an excellent way of accomplishing this. (アクセスを求める者が当人である事を確認するのが目的。例えば、jdoeというユーザー名のアカウントのパスワードが1234だとしたら、本当にJohn Doeがログインした保証はない。強いアカウントとパスワード変更の手順及び高いパスワード条件を設ける事で成しえる。二段階認証は特に効果的である)

# *Security Controls Explained in Plain English (Continued)*

**#7 Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse. (軍の契約に関する情報を保存した情報システム媒体は、破棄もしくは再使用する前に完全消去する)** This is another straight forward one, before disposing or releasing media from your control it should be sanitized or destroyed so that it is not recoverable by unauthorized persons. Media includes non-digital (paper, notebooks) and digital (i.e. thumb drives, hard disks, tape drives). Note: **NIST SP 800-88 (Rev-1) provides specific guidelines for sanitizing or destroying information system media containing "*federal contract information*" before disposal or release for reuse. See SP 800-88, Appendix G sample CERTIFICATE OF SANITIZATION (or go to http://csrc.nist.gov/publications).** (媒体を破棄したり手放す前に、認可されていない人物によりデータ復旧されないように完全消去する。非デジタルとデジタル媒体共に該当。 上記ウェブサイトに詳細あり)

**#8 Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals. (会社の情報システム、機器及びそれぞれの操作環境へのアクセスを認可された人に物理的に制限する)** Physical access to designated areas should be restricted (i.e. locked doors, locked cabinets) to authorized persons and the authorized persons should be identifiable (i.e. ID Card/badge) and documented. (認可された人による指定エリアへの物理的アクセスを制限する。鍵付きの扉やキャビネットなど。IDカード等で認可された人を確認できるようにする）

**#9 Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices. (来訪者はエスコートし行動を監視する。物理的アクセスのログを付け、アクセス用のデバイスを管理する)** Visitors should be escorted in sensitive areas where federal contract information is stored, a visitor sign in and exit sheet should be maintained. Proximity cards or other keys should be managed and updated to reflect changes in personnel access. (来訪者が軍との契約に関する情報が保管されている場所に立ち入る際はエスコートし、ログを記入する。アクセスする人が変わればスマートカードやその他の鍵をアップデートする)

# Security Controls Explained in Plain English (Continued)

**#10 Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. (通信の監視、管理及び保護)** This one is a bit wordy and seems complicated but it is essentially talking about maintaining firewalls and intrusion detection systems between your internal networks and the internet. You need to establish what the boundary of your information system is to properly implement this control. (内部ネットワークとインターネット間のファイヤーウォールや侵入検知システムを維持する。これらを適切に運用するために、情報システムの領域がどこなのかを定める必要がある。)

**#11 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. (物理的・論理的に内部ネットから隔離された外部からアクセス可能システムコンポーネント用のサブネットワークを使用する）**This control mandates that you implement what is known as a DMZ (Demilitarized Zone) to prevent traffic from the internet from reaching your internal network. Public facing systems should be placed in the DMZ and separated from your internal network either physically or via a firewall. (DMZと呼ばれるネットワーク領域を用いてインターネットから内部ネットワークへの侵入を防ぐ。外部に公開されたシステムはDMZに置きファイアウォール等で内部ネットワークと隔離する必要がある)

**#12 Identify, report, and correct information and information system flaws in a timely manner. (タイムリーに情報や情報システムの脆弱性を確認、報告及び是正する）**

This control requires that you patch vulnerabilities on your systems in accordance with your configuration management policies and procedures. Patching vulnerabilities should be done relatively quickly to avoid an attacker exploiting them. (システムの構成管理方針に従い、システムの脆弱点をパッチする事が必要。システムへの攻撃を防ぐため比較的すばやくパッチを行う必要がある)

# Security Controls Explained in Plain English (Continued)

**#13 Provide protection from malicious code at appropriate locations within organizational information systems. (悪意のあるコードから守るために情報システム内の適切な箇所で防御する）** This control requires that you maintain anti malware software on your systems. The phrase “appropriate locations” gives you an out if you can not install anti malware on systems such as servers due to technical constraints. (マルウェア対策ソフトをシステムに入れておく必要がある。システム上にマルウェア対策ソフトを入れられない場合はサーバー上)

**#14 Update malicious code protection mechanisms when new releases are available. (悪意のあるコードの防御機能は更新されたらアップデートする)** This means that you need to configure your anti malware software to update its anti-virus signatures so that it can detected the latest malware. (ウィルス対策シグネチャをアップデートするようにマルウェア対策ソフトを設定し、最新のマルウェアを検知できるようにする)

**#15 Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed. (情報システムは定期的にスキャンし、外部ソースからのファイルをダウンロード、開く、及び実行する際にリアルタイムスキャンする）** Your anti-malware software should be configured to periodically scan and to scan files in real time when downloaded or executed. It should also quarantine dangerous files and be able to disinfect your systems. (マルウェア対策ソフトは定期的にスキャンし、ファイルがダウンロードまたは実行される時にはリアルタイムスキャンするように設定しておく必要がある。危険なファイルを検疫し削除する事ができる)

# *Security Controls Explained in Plain English (Continued)*

In addition to the 15 security controls required by FAR 52.204-21, Defense contractors whose information systems process, store, or transmit "**covered defense information**" must also comply with Defense Federal Acquisition Regulation Supplement **(DFARS) clause 252.204-7012** – *Safeguarding Covered Defense Information and Cyber Incident Reporting*. (上記15の保安措置に加え、軍と契約を結ぶ業者で「対象国防情報」の処理、保管及び送信する情報システムを使用する業者はDFARSの条項252.204-7012に従わなければならない)

"**Covered defense information**" means unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government wide policies, and is— （「対象国防情報」とは法令法規により保護措置や公表管理が必要とされる技術情報及びその他情報を意味し）

(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or (契約履行のために、軍が契約業者に提供する契約書やタスクオーダーに記されているか)

(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract. (契約履行の為に、業者により収集、展開、受領、送信、使用または保管されている)

**To be compliant with DFARS clause 252.204.7012**, since December 31, 2017, **defense contractors have been required to implement the controls and policies that are set out in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 standards**. **Significantly, any defense contractor that submits a proposal in response to a solicitation that contains DFARS 252.204-7008 certifies compliance with the NIST SP 800-171 standards, which directly implicates the FCA**. (上記条項に準拠する為、軍の契約業者はNISTのSP800-171の基準に沿って管理しなければならない。特に、入札要件にDFARS規定252.204-7008を含むあんけんにたいして応札する軍の契約業者はNISTのSP800-171の基準を満たす事を保証する事になる)

# Potential Consequences of Noncompliance

- False Claims Act
- Suspension
- Debarment
- CPARS Evaluations

[redacted]

遵守しなかった場合の予想される結果：虚偽請求防止法、停止、禁止、評価

**The “**False Claims Act** (FCA)” is the primary weapon in combating fraud against the United States federal government. The FCA covers fraudulent claims made against any federal agency, program, contract, or grant. (FCA-虚偽請求防止法は連邦政府に対しての搾取に対しての最大の武器。政府機関、プログラム、契約もしくは補助金に対しての全ての請求に適用される)

**&#42;&#42;CPARS** is the Contractor Performance Assessment Reporting System

# Disclaimer

**The sole purpose of this REMINDER is to ensure industry is aware that Federal Acquisition Regulation (FAR) clause 52.204-21, Basic Safeguarding of Covered Contractor Information Systems, applies to all contracts, except COTS items, including contracts under the Simplified Acquisition Threshold AND that the clause includes fifteen (15) security controls that all contractors must meet in order to work with the federal government. These 15 security controls are designed to protect *federal contract information* (*FCI*) including *controlled unclassified information* (*CUI*) that contractors may handle over the course of their projects/contracts.**

***This Reminder is in no way intended to be interpreted as direction of any kind in complying with FAR 52.204-21 and does not substitute for vendor(s) seeking guidance from their own compliance professionals for advise concerning the clause and how to comply with the same.**

**This Reminder should not be considered a modification to any other Government contract.*

***This Reminder should not be used as an authoritative source for information concerning 48 CFR § 52.204-21. Consult the regulations for specific details and for changes on a regular basis.*

**This Reminder has been prepared for informational purposes only, and is not intended to provide, and should not be relied on for, cyber-security compliance advice. You should consult your own legal and/or cyber-security compliance advisors to determine if you are in compliance.**