REGULATION	FEDERAL REGISTER	APPLIES TO WHAT SYSTEMS?	APPLIES TO WHAT INFORMATION?	NIST STANDARD	INCIDENT DEFINED AS	MANDATORY INCIDENT REPORTING	REPORTING TIMELINE	COMPLIANCE ASSESSMENT/ CERTIFICATION	FEDRAMP
DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting. DFARS 252.204-7019 Notice of NISTSP 800-171 DoD Assessment Requirements. DFARS 252.204-7020 NIST SP 800-171DoD Assessment Requirements. DFARS 252.204-7021 Cybersecurity Maturity Model Certification Requirements	81 Fed. Reg. 72986 [1] 85 Fed. Reg. 61505	Any covered contractor information system, which is defined as "an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information." Focused primarily on requirements for nonfederal information systems, but also provides contractor requirements for protecting covered defense information on federal information systems. *See* DFARS 252.204-7012(b)(1) and (2).	Covered defense information ("CDI"), which is unclassified controlled technical information ("CTI") or other information, as described in the NARA CUI Registry and that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and government-wide policies, and is— (1) marked or otherwise identified, and provided to the contractor by or on behalf of DoD; or (2) collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.	NIST SP 800-171 Covered contractor information systems are subject to the security requirements in NIST SP 800-171 in effect at the time the solicitation is issued or as authorized by the Contracting Officer. Note that a Class Deviation issued in May 2024: DARS Tracking Number 2024-O0013 holds the NIST SP 800-171 revision to Revision 2 until further notice.	"Cyber incident" means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.	Report cyber incidents that affect a "covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract." Cyber incidents must be reported to the DoD at https://dibnet.dod.mil. Malicious software that a contractor or subcontractor discovers and isolates in connection with a reported cyber incident must be submitted to the DoD Cyber Crime Center in accordance with instructions provided by DC3 or the Contracting Officer. The contractor is required to provide, upon request, additional information or equipment for forensic analysis and damage assessment. This clause does not rescind other reporting obligations that the contractor may be under.	Cyber incidents must be reported within 72 hours of their discovery.	Basic, Medium, or High assessments are required in accordance with DFARS 252.204-7020 NIST SP 800-171 DOD Assessment Requirements. DFARS 252.204-7019 provides notice of NIST SP 800-171 DoD Assessment Requirements. DFARS 252.204-7021 sets forth compliance certification pursuant to Cybersecurity Maturity Model Certification (CMMC).	Under DFARS 252.204-7012, "[i]f the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline."
HSAR 3052.204-71 Contractor employee access. HSAR 3052.204-72 Safeguarding of controlled unclassified information. HSAR 3052.204-73 Notification and credit monitoring requirements for Personally Identifiable Information incidents.	88 Fed. Reg. 40560	Generally oriented toward federal information systems, which include contractor information systems used or operated on behalf of the agency. Requires adequate security, defined in the regulation, when: (1) contractor and/or subcontractor employees will have access to CUI; (2) CUI will be collected or maintained on behalf of the agency; or (3) federal information systems, which include contractor information systems operated on behalf of the agency, are used to collect, process, store, or transmit CUI.	Controlled Unclassified Information ("CUI"), defined in the regulation as "any information the Government creates or possesses, or an entity creates or possesses for or on behalf of the Government (other than classified information) that a law, regulation, or Governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls," and which includes information in 11 CUI categories and subcategories set forth in the regulation.	NIST SP 800-53. Regulations are silent on NIST SP 800–171 and nonfederal information systems, in deference to the NARA/FAR Council development of the CUI Rule.	*Incident* means an occurrence that— (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable-use policies.	Contractors and subcontractors shall report all known or suspected incidents to the Component Security Operations Center (SOC) in accordance with Attachment F, *Incident Response*, to DHS Policy Directive 4300A, *Information Technology System Security Program, Sensitive Systems*. For incidents involving PII/SPII, also provide as many of the data elements set forth in HSAR 3052.204-72(c)(5) as possible. Lower-tier subcontractors must also notify higher tiers until the prime contractor is reached, and the prime contractor must notify the Contracting Officer and COR. This clause does not rescind other reporting obligations that the contractor may be under.	All known or suspected incidents involving PII or SPII shall be reported within one hour of discovery. All other incidents shall be reported within eight hours of discovery.	HSAR 3052.204-72, Alt. I: When federal information systems are involved, the contractor must complete a Security Authorization process, and receive authority to operate. Contractors must also have an independent third-party assessment and validation of security and privacy controls in place for the information systems.	As this is a regulation for federal systems, FedRAMP is not explicitly and independently prescribed. However, in response to comments on the proposed rules, DHS stated that "[t]o the extent a contractor is proposing a cloud solution to the Department, DHS would comply with FedRAMP policies and procedures. This includes the expectation that contractors would rely on the documents the cloud service provider used to obtain its provisional ATO under FedRAMP and modify them to reflect any additional requirements necessary to provide the specific services required by the Department."

[1] DFARS 252.204-7012 was first proposed by an interim rule published in the Federal Register in 2013. The initial rule and DFARS clause was finalized in 2016, 81 Fed. Reg. 72986, and has since been subject to other updates. Additional clauses, DFARS 252.204-7019 through 7021, were added in 2020 by an interim rule, 85 Fed. Reg. 61505. For sake of simplicity, we reference only the 2016 final rule and the 2020 interim rule, except as otherwise expressly noted.

PROPOSED CUI RULE FAR 52.204-WW, Notice of Controlled Unclassified Information Requirements. FAR 52.204-XX, Controlled Unclassified Information. 52.204-YY, Identifying and Reporting Information That Is Potentially Controlled Unclassified Information.	90 Fed. Reg. 4278	Provides contractor requirements for both federal and nonfederal information systems. The proposed rule "introduces a new standard form (SF) to support uniformity in Governmentwide implementation of these policies. It identifies roles and responsibilities for agencies and contractors when controlled unclassified information (CUI) is located on Federal information systems within a Federal facility or resides on or transits through contractor information systems or within contractor facilities, and it adds two new clauses and a provision to enable contractor reporting and compliance responsibilities in Federal solicitations and contracts."	CUI that the government identifies in the SF XXX. Proposed addition to FAR 2.101 of a definition of CUI as "information that the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls," which excludes four categories of information set forth in the proposed rule.	NIST SP 800-53 (for Federal Information Systems) NIST SP 800-171 (for Non-Federal Information Systems) and the clause proposes holding at revision 2, as with the DFARS class deviation.	*CUI incident* is defined in FAR 52.204-XX and means improper access, use, disclosure, modification, or destruction of CUI, in any form or medium.	CUI in a federally controlled facility must be reported in accordance with agency policy. Suspected or confirmed CUI incidents in a non-federally controlled facility must be reported to the agency website or single point of contact identified in Part C, Section IV of the SF XXX. If no point of contact is defined in Form SF XXX, the FAR 52.204-XX requires reporting of as many of the applicable data elements located at https://dibnet.dod.mil/portal/intranet as possible within eight hours. Report unmarked or mismarked CUI and CUI incidents, but unmarked or mismarked CUI is not considered a CUI incident unless the mismarking or lack of marking has resulted in the mishandling or improper dissemination of the information.	Proposes eight-hour reporting requirement for CUI incidents in a non-federally controlled facility. Within a federally controlled facility, reports should be made in accordance with agency policy.	Contractors must cooperate with validation actions for nonfederal information systems, which the regulation establishes are "similar to the High Confidence Level Assessments being conducted by DOD pursuant to DFARS clause 252.204-7020, NIST SP 800-171 DoD Assessment." No mandated certification at present.	Contractors operating an information system identified as a federal information system that processes, stores, or transmits CUI must comply with agency-identified security controls from NIST 800-53. In addition, cloud service providers must meet security requirements established by the FedRAMP Moderate baseline. In regard to reporting requirements, if the contractor is a FedRAMP authorized cloud service provider, the contractor shall also report incidents to the point(s) of contact specified in the FedRAMP reporting guidelines as documented in the Cloud Service Provider Incident Response Plan.
FAR 52.204-21 Basic Safeguarding of Covered Contractor Information Systems. (Current requirements)	81 FR 30439	The existing clause provides contractor basic safeguarding requirements for protecting federal contract information on covered contractor information systems. A "covered contractor information system" is an information system that is owned or operated by a contractor that processes, stores, or transmits federal contract information.	*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 (such as on public websites) or simple transactional information, such as necessary to process payments."	Controls are loosely related to a subset of NIST SP 800-171 controls.	N/A	N/A	N/A	N/A	N/A
FAR 52.204-21 Basic Safeguarding of Covered Contractor Information Systems. (Requirements as proposed under the new CUI Rule)	90 Fed. Reg. 4278	"Covered contractor information system" is defined as "an information system owned or operated by a contractor on which the contractor processes, stores, or transmits covered Federal information."	Covered federal information, which is defined as information provided by or created for the government when that information is other than— (1) simple transactional information (such as that necessary to process payments); (2) information already publicly released (such as on public websites), or marked for public release, by the government; (3) federally funded basic and applied research in science, technology, and engineering at colleges, universities, and laboratories in accordance with National Security Decision Directive 189; (4) controlled unclassified information (CUI); or (5) classified information.	Controls are loosely related to a subset of NIST SP 800-171 controls.	N/A	N/A	N/A	N/A	N/A