SheppardMullin

Cybersecurity for Government Contractors

(Updated April 8, 2024)

If...?	FAR (Civilian Agencies)	DFARS (Dept. of Defense)	Vendor Management	Other Considerations
Contractor Information System processes, stores, or transmits **Federal Contract Information (FCI)**	15 basic security controls (FAR 52.204-21)	**Forthcoming:** Annual self-assessment against the 15 basic security controls and affirmation in SPRS (CMMC Level 1; DFARS 252.204-7021)	**Subcontract Flow-down:** Per FAR, when FCI may be residing in or transiting through subcontractor information system (except COTS)	**Individual agency contracts and subcontracts may have unique data security requirements and access restrictions*
Contractor Information System processes, stores, or transmits **Controlled Unclassified Information (CUI)**	**Forthcoming:** Implementation of the CUI Program through regulations for safeguarding and handling of CUI (FAR Case 2017-016)	Must have written System Security Plan (SSP) and Plan of Action & Milestones (POA&M) for NIST 800-171 and report cyber incidents within 72 hours (DFARS 252.204-7012) Perform a self-assessment (at least) against NIST 800-171 controls and report in SPRS (DFARS 252.204-7019/7020) **Forthcoming:** Perform self-assessment or Certification by a Third-Party Assessor Organization (C3PAO) (triennially), as specified in contract, against NIST 800-171 controls, and annual affirmation in SPRS (CMMC Level 2; DFARS 252.204-7021)	**Subcontract Flow-down:** Per DFARS 252.204-7012, when subcontract will involve covered defense information (i.e., CUI) or is for "operationally critical support" Per DFARS 252.204-7020, include in all subcontracts (except COTS) **Service Providers:** Per DFARS, contractor using an external cloud service provider (CSP) must ensure CSP is FedRAMP Moderate or equivalent and agrees to incident response requirements	Department of Homeland Security (DHS) – requires safeguarding and reporting of cyber incidents within 8 hours for CUI and within 1 hour for PII (HSAR 3052.204-71/72) Department of Veterans Affairs (VA) – requires protections for access to VA sensitive information, systems, and IT (Note "VA sensitive information" defined more broadly than CUI) (VAAR 852.204-71) **Individual agency contracts and subcontracts may have unique data security requirements and access restrictions*
Software developed by contractor available for purchase and used by federal agencies	**Forthcoming:** Software developers to attest to conformity with Secure Software Development Practices (FAR Case 2023-002)	N/A	Likely to be a flow-down component in forthcoming regulation Contractors will need to ensure software they provide or resell from third parties meets applicable requirements	CISA released a common Software Attestation Form in March 2024 Agencies directed to collect attestations for critical software within 3 months and for all other software within 6 months
Contractor provides or uses **Information and Communications Technology (ICT)** in performance of contract	**Forthcoming:** Contractors to report security incidents within 8 hours; share cyber threats; maintain Software Bill of Materials (SBOM); implement IPv6; allow access/cooperate with CISA/ agencies for threat hunting and response (FAR Case 2021-017)	N/A	Likely to be a flow-down component in forthcoming regulation SBOMs will require detailed records of the various components used in developing software	**Individual agency contracts and subcontracts may have unique data security requirements and access restrictions*

SheppardMullin

Cybersecurity for Government Contractors

(Updated April 8, 2024)

If...?	FAR (Civilian Agencies)	DFARS (Dept. of Defense)	Vendor Management	Other Considerations
Contractor operating a **Federal Information System** (i.e., operated "on behalf of" the Government) – ***Cloud***	**Forthcoming:** FedRAMP authorization at level determined by agency; for FedRAMP High systems, all Government data to be maintained within the U.S. unless otherwise specified (FAR Case 2021-019)	Contractors acting as cloud providers to DoD to comply with Cloud Computing Security Requirements Guide (SRG); maintain all Government data within the U.S. unless otherwise specified; report cyber incidents (DFARS 252.239-7010)	**Subcontract Flow-Down:** Per DFARS, where subcontracts involve or may involve cloud services Likely to be a flow-down component in forthcoming regulation	FedRAMP is the federal program for security authorizations for cloud offerings; FedRAMP authorization can be obtained for SaaS and other offerings not necessarily covered by the forthcoming FAR rule **Individual agency contracts and subcontracts may have unique data security requirements and access restrictions*
Contractor operating a **Federal Information System** (FIS) (i.e., operated "on behalf of" the Government) – ***Non-cloud***	**Forthcoming:** Contractors to comply with security obligations; records management and agency access to data and personnel; develop SSP; and conduct annual security assessments; among other requirements (FAR Case 2021-019)	N/A	Likely to be a flow-down component in forthcoming regulation	Generally, agencies will require implementation of a subset of the controls in NIST 800-53 based on FIPS 199 categorization **Individual agency contracts and subcontracts may have unique data security requirements and access restrictions*
Covered Critical Infrastructure entities – large businesses in 16 industry sectors and small businesses in select sectors based on specified criteria		**Forthcoming:** New regulations from CISA under the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) will require reporting of substantial cyber incidents to CISA within 72 hours and ransom payments within 24 hours Covered entities specifically include DoD contractors subject to DFARS 252.204-7012, government IT providers, and "critical software" developers		
Public Companies		Per SEC regulations, must disclose material cybersecurity incidents within 4 business days of materiality determination and provide other disclosures **Potential to delay reporting, if authorized by DOJ, for national security or public safety*		

Washington, D.C. Governmental Practice Cybersecurity & Data Protection Team:

Townsend Bourne
Partner, Team Leader
tbourne@sheppardmullin.com

Nikki Snyder
Associate, Team Deputy
nsnyder@sheppardmullin.com

Dany Alvarado
Associate
dalvarado@sheppardmullin.com

Lily Damalouji
Associate
ldamalouji@sheppardmullin.com

Jordan Mallory
Associate
jmallory@sheppardmullin.com

Learn more about the Governmental Practice Cybersecurity & Data Protection Team