52.240-93 BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORMATION SYSTEMS (NOV 2025) (DEVIATION)

(a) Definitions. As used in this clause—

Covered contractor information system means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.

Federal contract information—

(1) 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

(2) Does not include information provided by the Government to the public (such as on public websites) or simple transactional information (such as information necessary to process payments).

Information means any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual (Committee on National Security Systems Instruction (CNSSI) 4009).

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502).

Safeguarding means measures or controls that are prescribed to protect information systems.

(b) *Safeguarding requirements*.

(1) Basic requirements. The Contractor shall safeguard its covered contractor information systems by implementing, at minimum, the following security controls:

(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

(iii) Verify and control/limit connections to and use of external information systems.

(iv) Control information posted or processed on publicly accessible information systems.

(v) Identify information system users, processes acting on behalf of users, or devices.

(vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

(vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

(viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

(ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.

(x) 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.

(xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

(xii) Identify, report, and correct information and information system flaws in a timely manner.

(xiii) Provide protection from malicious code at appropriate locations within organizational information systems.

(xiv) Update malicious code protection mechanisms when new releases are available.

(xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

(2) Other requirements. This clause does not relieve the Contractor of any other specific safeguarding requirements specified by Federal departments and agencies relating to covered contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information (CUI) as established by Executive Order 13556.

(c) Subcontracts. The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts under this contract (including subcontracts for the acquisition of commercial products, other than commercially available off-the-shelf items, or commercial services), in which the subcontractor may have Federal contract information residing in or transiting through its information system.

(End of clause)