ASSESSING THE STATE OF A CONTRACTOR'S INTERNAL INFORMATION SYSYEM IN A PROCUREMENT ACTION

	OBJECTIVE	SOLICITATION/RFP	SOURCE SELECTION	CONTRACT
1.	Evaluate implementation of NIST SP 800-171* at source selection	• DFARS Provision 252.204-7008 • DFARS Clause 252.204-7012		• DFARS Clause 252.204-7012
	Alternative 1A.: Go/No Go decision based on implementation status of NIST SP 800-171*	• RFP (e.g., Section L) must require delivery of NIST SP 800-171 Security Requirement 3.12.4 - System Security Plan (or specified elements of) with the contractor's technical proposal • RFP (e.g., Section L) must require delivery of NIST SP 800-171 Security Requirement 3.12.2 - Plans of Action with the contractor's technical proposal • RFP (e.g., Section M) must identify requirements for an "Acceptable" (Go/No Go threshold) rating. [See Resources: DoD Guidance for Reviewing System Security Plans]	• Evaluate NIST SP 800-171 Security Requirement 3.12.4 - System Security Plan (or specified elements of) and any NIST SP 800-171 Security Requirement 3.12.2 - Plans of Action, in accordance with Section M [See Resources: DoD Guidance for Reviewing System Security Plans]	• Incorporate NIST SP 800-171 Security Requirement 3.12.4 - System Security Plan (or specified elements of) and any NIST SP 800-171 Security Requirement 3.12.2 - Plans of Action as part of contract

	OBJECTIVE	SOLICITATION/RFP	SOURCE SELECTION	CONTRACT
1.	Alternative 1B. Assess NIST SP 800-171* implementation as a separate technical evaluation factor	• RFP (e.g., Section M) must identify how implementation of NIST SP 800-171* will be evaluated. Evaluation may consist of one or both of the following:	• Evaluate implementation of NIST SP 800-171* in accordance with RFP (e.g., Section M)	• Incorporate System Security Plan (or specified elements of) and any Plans of Action as part of contract
		– Assess based on NIST SP 800-171 Security Requirement 3.12.4 - System Security Plan (or specified elements of)	– See Resources: DoD Guidance for Reviewing System Security Plans	
		– Validate implementation for the competitive range with an independent government assessment in accordance with NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information	– See Resources: NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information	

	OBJECTIVE	SOLICITATION/RFP	SOURCE SELECTION	CONTRACT
2.	Require protections in addition to the security requirements in NIST SP 800-171 and evaluate at source selection	• DFARS Provision 252.204-7008 • DFARS CLause252.204-7012 • RFP (e.g., Sections H and L) will identify requirements in addition to NIST SP 800-171 • RFP (e.g., Section M) will detail specifics of how additional requirements will be evaluated • See also 1A and 1B above	• Evaluate offeror's proposed implementation of protections required in addition to NIST SP 800-171 in accordance with RFP (e.g., Section M) • See also 1A and 1B above	• DFARS Clause 252.204-7012 • Include SOW language describing additional requirements • See also 1A and 1B above

	OBJECTIVE	SOLICITATION/RFP	SOURCE SELECTION	CONTRACT
3.	Assess/track implementation of NIST SP 800-171* security requirements after contract award	• DFARS Provision 252.204-7008 • DFARS Clause 252.204-7012 • RFP (e.g., Section L) must require delivery of NIST SP 800-171 Security Requirement 3.12.4 - System Security Plan (or specified elements of) with the contractor's technical proposal • RFP (e.g., Section L) must require delivery of NIST SP 800-171 Security Requirement 3.12.2 - Plans of Action with contractor's technical proposal • RFP (e.g., Sections H and L) must include contract data requirements (using DD 1423, Contract Data Requirements List) to require implementation of Plans of Action to require delivery of System Security Plan and any Plans of Action after contract award. • In addition to the above – the RFP may also identify requirement for periodic reporting of results of continuous monitoring per NIST SP 800-171 Security Requirement 3.12.3		• DFARS Clause 252.204-7012 • Include SOW language and data requirement in the Contract Data Requirements List requiring delivery of System Security Plan and any Plans of Action after contract award • Incorporate System Security Plan (or specified elements of) and any Plans of Action as part of the contract • Include appropriate SOW language and a data requirement in the Contract Data Requirements List requiring implementation of any Plans of Action • Include appropriate SOW language and data requirement in Contract Data Requirements List indicating DoD will track implementation of Plans of Action • Include appropriate SOW language and a data requirement in the Contract Data Requirements List requiring periodic reporting of continuous monitoring results when applicable

	OBJECTIVE	SOLICITATION/RFP	SOURCE SELECTION	CONTRACT
3.	The government may also monitor compliance of NIST SP 800-171* with independent government assessment	• RFP (e.g., Sections H and L) must indicate if and how the government will monitor compliance of NIST SP 800-171* with independent government assessment in accordance with NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information[See Resources]		• Include requirement for the contractor to support independent government assessment of compliance of NIST SP 800-171* in accordance with NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information [See Resources]

	OBJECTIVE	SOLICITATION/RFP	SOURCE SELECTION	CONTRACT
4.	Contractors 'self-attest' to compliance with DFARS 252.204-7012 and implementation of NIST SP 800-171*	– DFARS Provision 252.204-7008 – DFARS Clause 252.204-7012		– DFARS Clause 252.204-7012

* When 'adequate security' requires security measures in addition to the NIST SP 800-171 security requirements (determined as necessary by the contractor), these additional measures will be evaluated and monitored in a manner similar to the NIST SP 800-171 requirements. Plans of action, continuous monitoring and the system security plan (NIST SP 800-171 Security Requirements 312.2-3.12.4) must address all security requirements.

REFERENCES/RESOURCES
DFARS Provision 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls — Requires that the Offeror represent that it will implement the security requirements specified by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations."
DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting — Requires contractors to provide "adequate security" for covered defense information that is processed, stored, or transmitted on the contractor's internal information system or network. To provide adequate security, the contractor must, at a minimum, implement National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations."

REFERENCES/RESOURCES (continued)

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations" — Provides federal agencies with a set of recommended security requirements for protecting the confidentiality of CUI when such information is resident in nonfederal systems and organizations; when the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or government-wide policy for the CUI category or subcategory listed in the CUI Registry. The security requirements apply to all components of nonfederal systems and organizations that process, store, or transmit CUI, or that provide security protection for such components. The requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations.

Documenting Implementation of NIST SP 800-171 — Companies should have a **system security plan** in place, in addition to any associated **plans of action** to describe how and when any unimplemented security requirements will be met, how any planned mitigations will be implemented, and how and when they will correct deficiencies and reduce or eliminate system vulnerabilities

- **NIST SP 800-171 Security Requirement 3.12.4 (System Security Plan)** — Requires contractor to develop, document, and periodically update, system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems
- **NIST SP 800-171 Security Requirement 3.12.2 (Plans of Action)** — Requires contractor to develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in their systems

DoD Guidance for Reviewing System Security Plans – Developed to:

- Facilitate the consistent review and understanding of System Security Plans and Plans of Action, and the impact that NIST SP 800-171 Security Requirements that are not yet implemented have on an information system.
- Assess the risk that a security requirement left unimplemented has on an information system
- Assess the risk of a security requirement with an identified deficiency
- Address the priority for which an unimplemented requirement should be implemented

NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information –

- Provides federal and nonfederal organizations with assessment procedures and a methodology that can be employed to conduct assessments of the CUI security requirements in NIST SP 800-171
- Intended to help organizations develop assessment plans and conduct efficient, effective, and cost-effective assessments of the security requirements in NIST SP 800-171

Note (to be removed later): NIST SP 800-171A is in Final Public Draft (comments due March 23 with expected publication in May)