Including Cybersecurity in the Contract Mix

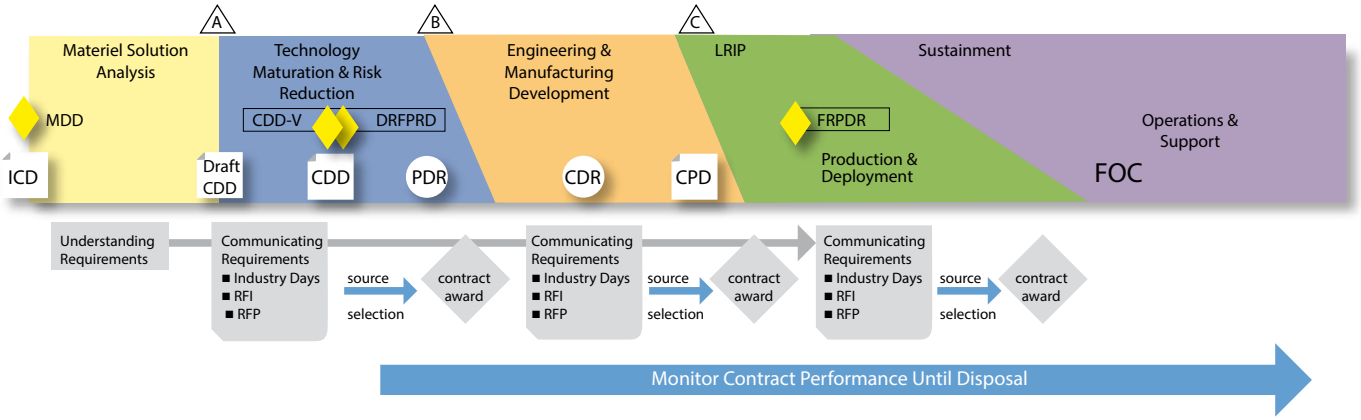
Kimberly L. Kendall ■ *William E. Long, Jr.*

Cybersecurity is a team sport that requires Program Management, Cyber/Information Technology, Engineering, Test and Evaluation, Finance, Logisticians and Contracting. In order to improve the survivability of our Department of Defense (DoD) systems under cyberattack, we must consider cybersecurity in the earliest phases of contract planning—from acquisition planning to contract maintenance and closeout.

If cybersecurity isn't properly integrated into the solicitation process we won't (1) know if the offerors are capable of delivering our cybersecurity requirements, (2) be able to discriminate between offeror proposals or (3) be able

Kendall *and* **Long** *are professors, respectively, of cybersecurity and contract management at the Defense Acquisition University's South Region in Huntsville, Alabama. Kendall, a retired Air Force colonel, is a former deputy division chief for Information Technology/Cyber Programs, Air Staff Information Dominance Directorate, Office of the Assistant Secretary of the Air Force for Acquisition. Long also performs consulting efforts for the Department of Defense and other federal agencies and participates as a subject-matter expert ensuring curriculum currency and enhancing processes within the contracting career field. He is the course manager for DAU's Contingency Contracting Course, CON 234.*

Figure 1. Contracting Touchpoints Across the Acquisition Life Cycle



Key to Figure: ICD=Initial Capabilities Document; CDD=Capability Development Document; CDD-V=Capability Development Document Validation; CPD=Capability Production Document; CDR=Critical Design Review; DRFPRD=Development Request for Proposals Release Decision; FOC=Full Operational Capability; FRPDR=Full-Rate Production Decision Review; LRIP=Low-Rate Initial Production; MDD=Materiel Development Decision; PDR=Preliminary Design Review; RFI=Request for Information; RFP=Request for Proposal

Source: Adapted by authors from DAU's Cybersecurity and Acquisition Life-cycle Integration Tool

to provide the proper oversight since we may not have asked for the appropriate data to monitor contract performance. Ensuring cybersecurity is appropriately addressed in the solicitation process involves more than selecting Federal Acquisition Regulation (FAR)-Defense Federal Acquisition Regulation Supplement (DFARS) clauses!

Cybersecurity requirements, like other system requirements, underpin the solicitation process. Early involvement by the contracting officer is the key to successful incorporation of cybersecurity requirements into the Request for Proposal (RFP), source selection and post-award contractor execution activities. Additionally, contracting officers need to understand a program's cybersecurity requirements and risks to inform contract type selection. Figure 1 shows touch points in the life cycle where contracting solicitation activities should include cybersecurity considerations.

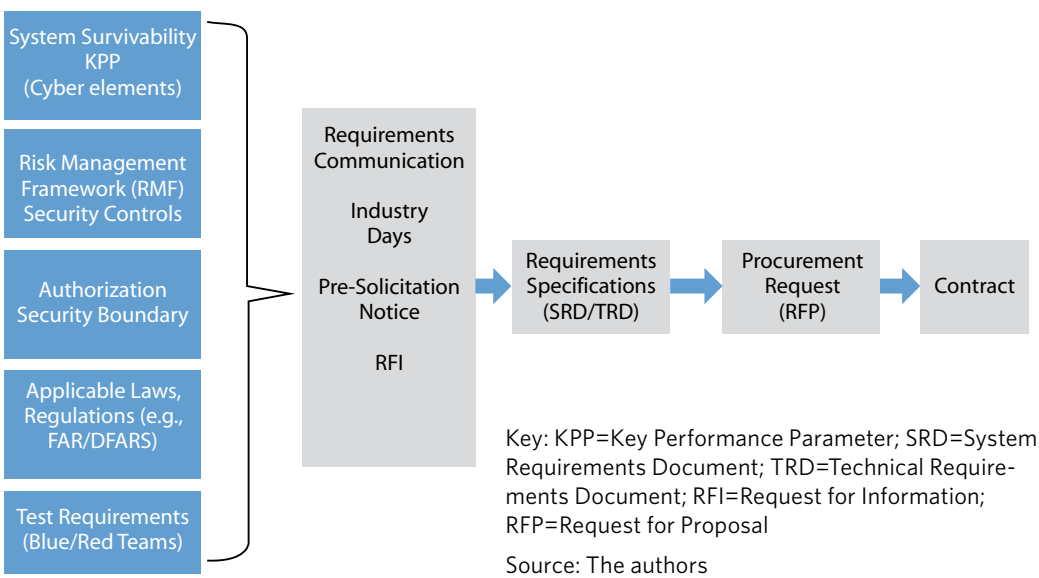
Understanding and Communicating Requirements

Contracting for cybersecurity begins in the Requirements Phase. It is imperative that the contracting officer understand the program's cybersecurity requirements and construct a contracting strategy to determine whether offerors are capable of delivering those requirements.

Many cybersecurity requirements are included in the mandatory System Survivability Key Performance Parameter (KPP) because Cyber Survivability is now a key element. All cybersecurity-required capabilities (including those derived from the Risk Management Framework [RMF] process) are decomposed into the government-owned technical requirements baseline. Traceability and balance between cybersecurity requirements, security controls and mission needs is of critical importance. This is where the contracting officer can help the program manager (PM) make informed trade-space decisions.

Cybersecurity requirements should be communicated with industry through various forums (e.g., Industry Days, Sources

Figure 2. Putting Cybersecurity Requirements on Contract



Key: KPP=Key Performance Parameter; SRD=System Requirements Document; TRD=Technical Requirements Document; RFI=Request for Information; RFP=Request for Proposal

Source: The authors

Sought Synopsis, Request for Information (RFI), one-on-one meetings, Draft RFP, Preproposal Conferences, etc.) and ultimately included in the final RFP. This will provide industry with a better understanding of the breadth and depth of cybersecurity requirements. See Figure 2.

Source Selection

Clearly communicated cybersecurity requirements provide potential offerors information on which to base their proposed solutions and provide DoD with measures to evaluate offeror capability and solutions. Cybersecurity risk should be a consideration when determining evaluation criteria to provide discriminators among proposals. The following are just a few resources providing examples of cybersecurity considerations that can be incorporated into the RFP: the DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle; the Guide for Integrating Systems Engineering into DoD Acquisition Contracts; Suggested Language to Incorporate System Security Engineering for Trusted Systems and Networks into DoD Requests for Proposals; and https://shortcut.dau.mil/ncma/cyber_contracts. Table 1 is a sampling of these considerations.

FAR/DFARS Clauses and Public Law

The procurement team should work together, but the contracting officer has the ultimate responsibility for FAR and the Defense FAR Supplement (DFARS) requirements. DoD Instruction (DoDI) 5000.02, Change 3, Enclosure 14, specifically calls out the following:

- FAR Clause 52.204-2 Security Requirements
- FAR Clause 52.204-21 Basic Safeguarding of Covered Contractor Information Systems
- Section 933, National Defense Authorization Act, FY [Fiscal Year] 2013, Public Law 112-239—Improvements in Assurance of Computer Software Procured by the Department of Defense
- DFARS Clause 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting
- Section 937, National Defense Authorization Act, FY 2013, Public Law 113-66—Joint Federated Center for Trusted Defense Systems for the Department of Defense

Additional cybersecurity-related DFARS clauses include:

- DFARS Clause 252.204-7008—Compliance with Safeguarding Covered Defense Information Controls
- DFARS Clause 252.204-7009—Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information
- DFARS Clause 252.239-7009—Representation of Use of Cloud Computing
- DFARS Clause 252.239-7010—Cloud Computing Services
- DFARS Clause 252.239-7017—Notice of Supply Chain Risk
- DFARS Clause 252.239-7018—Supply Chain Risk

The foregoing is not an all-inclusive, one-size-fits-all list, and contracts should be based on individual program requirements and risk!

Effective Cybersecurity Government Oversight

To determine if cybersecurity requirements are being implemented effectively, the right data and tools need to be written into the contract. The following are examples of data, artifacts and/or activities that we might monitor:

- Software vulnerability scans (static and dynamic)
- Formal code inspections
- Software quality measures and configuration control
- Test coverage

Incentivize Cybersecurity Performance

Incentives are fundamental elements of any contract. The contract itself motivates successful performance from a monetary standpoint, future relevant work and "brand" reputation. However, since cybersecurity historically has been treated as a compliance checklist, perhaps we need to incentivize contractor efforts beyond "check the box" minimum performance by incorporating specific incentives designed to encourage exceptional performance. In the face of ever-increasing cyber threats, cybersecurity may be a critical risk area necessitating extra effort to mitigate those risks.

There can be a combination of financial and nonfinancial incentives, including improved cash flow, increased business

Table 1. Request for Proposal (RFP) Sample Cybersecurity Considerations

Request for Proposal	
Section B	Supplies or services and prices/costs • Review all CDRL deliverables for inclusion of cybersecurity execution support (e.g., data rights, test data, test plans, source code deliveries, prototype quantity, and delivery times and/or locations).
Section C	Description/Specification/Statement of Work • State—in performance-based terms—cybersecurity requirements levied on the contractor. • Include cybersecurity system/technical requirements in the SRD/TRD. • Identify the system RMF categorization, overlays, RMF security controls to inform scope. • Identify any specific design, contractor testing or artifacts that enable compliance with cybersecurity requirements.
Section E	Inspection and acceptance • Ensure that a quality assurance surveillance plan exists to monitor contractor performance, including cybersecurity.
Section F	Deliveries or performance • Ensure that cybersecurity-related items are addressed like any other type of requirement (e.g., test article delivery, contractor support for repair, etc.).
Section H	Special contract requirements • List applicable cybersecurity special contract requirements (e.g., handling of data, software license management and maintenance, use of contractor facilities for cybersecurity testing).
Seciton I	Contract clauses • Cybersecurity-specific contract clauses should be considered.
Section J	List of attachments • Consider applicable cybersecurity attachments (e.g., a DoD component RMF Guide, Program Protection Plan).
Section K	Representations, Certifications, and Other Statements of Offerors or Respondents • Include requests for certification that support the cybersecurity strategy (e.g., National Security Agency certifications of cryptographic algorithms or equipment, and certification of cross domain solutions).
Section L	Instructions, Conditions, and Notices to Offerors or Respondents • Describe the experience of cybersecurity staff, predicted staffing levels, and the application of cybersecurity best practices and its alignment with the contractor management structures for SSE and T&E. • Define the contractor's responsibilities for cybersecurity and the alignment of those responsibilities in contrast to the government for required SSE and T&E activites (e.g., contractor cybersecurity testing, developmental testing, and integrated testing). • Describe the contractor's approach for technical data, including management, ownership, control, timely access, and delivery of all cybersecurity data, including raw test data, to support the evolving technical baseline. • Define CDRLs and select applicable DIDs. Identify any cybersecurity-related data products contractors must provide. • Describe contractor's approach for satisfying the Program Protection Plan. • Describe contractor's approach for detecting counterfeit components and use of cyber-certified products for hardware and software. • Describe the contractor's access to government cyber ranges, use of commercial and/or government Blue and/or Red teams during cybersecurity testing.
Section M	Evaluation Factors for Award • Prior performance in integrating cybersecurity considerations into the program's SE, SSE and T&E processes. • Meet cybersecurity workforce certification and training requirements in DoDD 8140.01 and DoD 8570.01-M, and investigative requirements per DoDI 8500.01. • Prior support to government achieving cost-effective cybersecurity authorizations to operate. • Define measures and metrics clearly to evaluate qualification of contractor cybersecurity staff. • Degree to which cybersecurity is included in design trade analysis. • Degree to which security testing is integrated into software development. • Degree to which supply chain risk management ensures security and integrity of sourced components. • Degree to which supply chain diversity is implemented.

Key to Table: CDRL=Contract Data Requirements List; DID=Data Item Description; DoDI=DoD Instruction; DoDD=DoD Directive; RMF= Risk Management Framework; SE=Systems Engineering; SRD=System Requirements Document; SSE=Systems Security Engineering; T&E=Test and Evaluation; TRD=Technical Requirements Document.

Sources: *DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle*; the G*uide for Integrating Systems Engineering into DoD Acquisition Contracts*; *Suggested Language to Incorporate System Security Engineering for Trusted Systems and Networks into DoD Requests for Proposals*; and https://shortcut.dau.mil/ncma/cyber_contracts.

base and stable workforce employment. Incentives also can be either positive, negative or a combination of both. They should be applied selectively to motivate contractor efforts that otherwise might not be emphasized and to discourage suboptimal performance.

When it comes to incentives, we must always strive to have a better understanding of what incentives do and make sure that we're incentivizing the correct behavior. Early market research is the key to doing this successfully. For one thing, in using multiple incentive arrangements, we need to ensure that we always include a cost incentive so that the contractor doesn't exceed contractual costs by chasing that incentive. We also need to ensure that multiple incentives are not driving suboptimal performance in other areas—or contradicting one another.

The development of an effective acquisition strategy begins with understanding the program's cybersecurity requirements and making a thorough evaluation of risk. Contract incentives must properly motivate the contractor. Hence, we must understand factors that are most important to the contractor.

Contract Type Challenges for Cybersecurity

Factors to consider when selecting a contract type include (1) performance risk and uncertainty, (2) urgency, complexity and stability of the requirement, (3) competition and (4) technology maturity. A challenge for cybersecurity is the availability of historical cost and pricing data as we build cybersecurity into the design of systems as opposed to using a previous compliance checklist approach. The ever-increasing cyber threat drives up uncertainty as new vulnerabilities are discovered daily. As we tackle this threat, the contract type needs to give us the flexibility to make adjustments as we learn what is feasible and affordable.

Summary

The contracting community has a crucial role to play in ensuring cybersecurity requirements are effectively included in the contract. This starts with gaining a complete understanding of the program requirements so that the solicitation can be effectively constructed to differentiate between competing offerors' proposals and determine their capability to deliver cybersecurity. The program management office needs to effectively communicate requirements to industry partners so they understand the scope of those requirements. This cannot be done effectively without early engagement on the part of the contracting officer.

The authors can be contacted at **kim.kendall@dau.mil** *and* **william.long@dau.mil**.