Information technology campaigns by adversaries of the United States threaten our national security. These campaigns use social media, artificial intelligence, data analysis, encryption technologies, and cyber attacks. These technologies and attacks continue to evolve and advance.

According to an unclassified December 2018 Government Accountability Office (GAO) report, the United States faces a complex array of threats to our national security that will continue changing as our adversaries become more technologically proficient. The report reviewed approximately 210 individual threats and identified 26 long-range emerging threats—those that may occur in 5 or more years or within an unknown timeframe. Those identified had a national security consequence, including adversaries’ political and military advancements, dual-use technologies, weapons, and geopolitical events.
On July 20, 2020, then-Defense Secretary Mark T. Esper issued a memorandum announcing a campaign to change a culture of inadequate Operations Security practices and habits within the Department of Defense (DoD). The memorandum, titled, “Reinforcing Operations Security and the Importance of Preventing Unauthorized Disclosures,” emphasized the critical nature of unauthorized disclosure or “leaks” of classified national security information that would have an injurious effect on DoD personnel, operations, strategies, and policies to the benefit of U.S. adversaries.

Information owned by or under the control of the U.S. Government may be classified to protect national security only if its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to national security. Unauthorized disclosure of classified information to an unauthorized recipient is a violation of U.S. law and can involve publication or other means of distribution.

Protection of classified information is a responsibility that dominates all Army and DoD employees, both military and civilian. And when national security is compromised—when our nation’s secrets are inadvertently or inadvertently disclosed—it may result in serious, grave, or exceptionally grave damage to the safety, security, and defense of the United States.

Full and open competition is the general rule of the Competition in Contracting Act when soliciting offers for government contracts. But there are limited national-security exceptions.

Restrictions under a national security exception are permissible under Federal Acquisition Regulation (FAR) 6.302-6 when disclosing the government’s needs would compromise national security. However, under the statutory exception, agencies still must request offers from as many potential sources as is practicable.

Of particular concern to acquisition officials is the disclosure of classified information to commercial sources, information fundamental to contract performance in order to satisfy the government’s requirements. The government’s needs must be articulated without ambiguity in soliciting offers while protecting U.S. secrets from unauthorized disclosure.

Yet, under the FAR provision and the various defense directives and instructions, what constitutes a compromise of national security in soliciting the government’s procurement needs? What security requirements would be violated by disclosure of the government’s needs? What information is “classified” for soliciting bids or proposals? And, since the national security exception requires that agencies request offers from as many potential sources
as is practicable, should disclosure of the government’s classified procurement requirements be released to any potential offeror possessing a clearance level equivalent to that information?

(1) What constitutes a compromise of national security?
(Point: Not classified, no compromise. Acquisition documents often claim information is classified without providing supporting evidence. The U.S. Marshalls decision outlined below illustrates that point.)

A compromise of national security occurs when the nation’s classified information is either knowingly and willfully or negligently disclosed.

When soliciting offers for the government’s procurement needs, the contracting officer must determine whether prospective offerors will require access to classified information. Information cannot be classified simply in order to restrict competition. The information, then, first must be classified in order before a compromise of national security can occur.

This may be obvious, but it is important to recognize that the national security exception to full and open competition applies unless disclosure of the procurement needs is not expected to compromise the national security. It is a fallacy to assume that the government’s information is classified merely because the information appears too sensitive to be released and should be safeguarded by limiting competition. Information necessary for contract performance must be classified for the national security exception to apply.

In 1986, the U.S. Marshals Service initiated a procurement for equipment that would detect weapons and explosives placed in federal buildings and courthouses throughout the United States. The contracting officer for that procurement executed a justification and approval for other than full and open competition under the national security exception. The contracting officer then issued the unclassified solicitation to a limited number of firms. A protest soon followed to the then General Accounting Office (renamed the Government Accountability Office in 2004, and always known as the GAO).

The GAO found that the contracting officer unnecessarily relied on the national security exception because the solicitation included both the required performance capabilities as well as the salient characteristics of the detection equipment being procured. The GAO concluded that disclosure of the procurement to other firms would not have compromised the national security. See GAO B-224258, Feb. 4, 1987.

It is a violation of procurement regulations to restrict competition based on the national security exception when the information necessary for contract performance does not compromise national security.

(2) What security requirements would be violated by disclosing the government’s needs?
(Point: The Security Classification Guide (SCG) conforms to classification requirements and standards in Army Regulation (AR) 380-5 and DoD regulations.)
FAR 6.302-6, National Security, applies when disclosure of the government’s needs would, for example, violate security requirements.

Numerous regulations and manuals address security requirements. For example, DoD Instruction (DoDI) 5200.01 requires national security information to be classified, safeguarded, and declassified in accordance with DoD Manual 5200.01. According the manual, information shall be classified only when necessary in the interests of national security. Access to national security information may be granted to people who have both the appropriate security clearance and a valid need-to-know in order to perform a lawful and authorized governmental function. DoDI 5200.01 requires that classified information released to industry must be safeguarded in accordance with DoDI 5220.00. FAR 4.403(a) requires contracting officers to review all proposed solicitations to determine whether access to classified information may be required by offerors.

What document identifies the conditions for releasing classified information without violating security requirements?

The SCG is the primary document that identifies the specific government-owned information that must be protected from unauthorized disclosure to protect the national security.

AR 380-5 explains that an SCG will be issued for each system, plan, program, project, or mission involving classified information. The SCG conforms to standards included in AR 380-5 and DoD regulations issued under DoDM 5200.01, Volume 1.

The SCG identifies specific items or elements of information to be protected and the classification level to be assigned each item or element.

(3) What information is “classified” in soliciting bids or proposals?

(Point: Some portions of the requirement may be classified and some not based on the SCG.)

Of primary concern to acquisition officials is the authorized disclosure of classified information to commercial sources to satisfy the government’s requirements when classified information is fundamental to contract performance.

The authority to classify information may be exercised only by specifically authorized individuals, usually by an Original Classification Authority (OCA).

The SCG communicates the decision by the OCA to designate certain information as classified, at a particular level, and for a particular duration of time.

The SCG establishes classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified, the associated classification level—e.g., Confidential, Secret, Top Secret—and duration of classification for each element.

A particular government procurement requirement may include both classified and unclassified specifications or elements that describe the government's procurement need. The SCG will identify those specifications or elements that must be protected from unauthorized disclosure.

Competition must not be limited merely because the acquisition is classified, or merely because access to classified matter will be necessary to submit a proposal or to perform the contract. Competition may be limited only to the extent necessary to satisfy the needs of the agency or as authorized by law. Consistent with the SCG's provisions, and in order to promote full and open competition, the contracting officer must describe the government’s procurement needs in such a way that the solicitation would not disclose U.S. secrets or compromise national security.

To demonstrate that disclosure of the government’s needs would compromise national security, the Justification and Approval (J&A) documenting the decision to limit full and open competition must identify the applicable SCG by title and date. It must show a determination that disclosure of the specific classified information must be restricted to protect national security.
(4) Should procurement requirements be disclosed to any potential offeror having an equivalent clearance level?
(Point: Understand the importance of need-to-know.)

Acquisition officials must articulate the government’s needs to prevent the divulging of our nation’s secrets, and at the same time, solicit offers “from as many potential sources as is practicable under the circumstances,” according to the national security exception of Federal Acquisition Regulation (FAR) 6.302-6.

Unquestionably, many interested contractors may have the personnel and facilities authorized to receive classified information and may concurrently be actively engaged in performing similar, highly classified work—perhaps at levels far higher than the classification applied to the government’s current requirement.

The Defense FAR Supplement Procedures, Guidance and Instruction (DFARS PGI) states that contracting officers must ensure that solicitations requiring offerers’ access to classified information include one or more of the following:

- A draft Department of Defense (DD) Form 254, DoD Contract Security Classification Specification
- The Security Requirements clause at FAR 52.204-2
- Detailed instructions on how offerors may request access to the classified information

The DD Form 254 is used to convey security requirements to contractors when contract performance requires access to classified information.

The Security Requirements clause at FAR 52.204-1 essentially requires that the successful contract award winner comply with the DD Form 441 Security Agreement and the National Industrial Security Program Operating Manual, DoD 5220.22-M.

Should possession of the required personnel and facility clearances permit an individual or entity unconditional access to classified procurement information?

In 2016, the Air Force issued a classified J&A for award of a sole-source contract to L3 Technologies based on the national security exception at FAR 6.302-6. The Boeing Company challenged the Air Force’s J&A in a protest to the GAO, arguing that the national security exception in the J&A unreasonably relied on a finding that the classified information to which L3 has access could not be shared with America’s Warfighters depend on the security of information in competitively issued contracts to supply their needs.
other contractors. The Boeing protest noted that Boeing had the personnel and facilities to receive the classified information and that work it previously performed for the government involved far higher classifications than the Secret level applied in the J&A.

The GAO denied Boeing’s protest of the J&A after concluding that the Air Force reasonably made a need-to-know determination that precluded the transfer of classified information to an additional contractor. See GAO B-414706; B-414380.2, Aug. 25, 2017.

Access to classified information is allowed only to individuals who possess a valid and appropriate security clearance; have executed an appropriate non-disclosure agreement; and have a valid need-to-know in order to perform a lawful and authorized government function.

According to AR 380-5, Army personnel are personally responsible to ensure that those seeking access to classified information have the necessary security clearance before authorizing that access. And the holder of classified information must confirm that there also is a valid “need-to-know” before disclosing that information.

Need-to-know is a determination by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function. Need-to-know provisions may preclude the clearance of additional sources for solicitation and performance of work, even to those sources that might possess access to information classified at equivalent or higher levels on other programs.

When competition is limited based on the national security exception and need-to-know provisions, the J&A must explain the need-to-know restriction if access by commercial sources to classified information is fundamental to contract performance.

**Conclusion**

Limiting competition for federal contracting opportunities based on national security is not solely a matter of keeping secrets safe but also of recognizing what actions or omissions may or may not compromise national security when soliciting the government’s procurement needs. The SCF is the primary document that identifies and regulates disclosure of classified information for soliciting bids or proposals. Understanding need-to-know requirements before disclosing the government’s classified procurement requirements will avoid an unlimited and unauthorized release of classified information to any potential offeror possessing a clearance level equivalent to the information being disclosed.