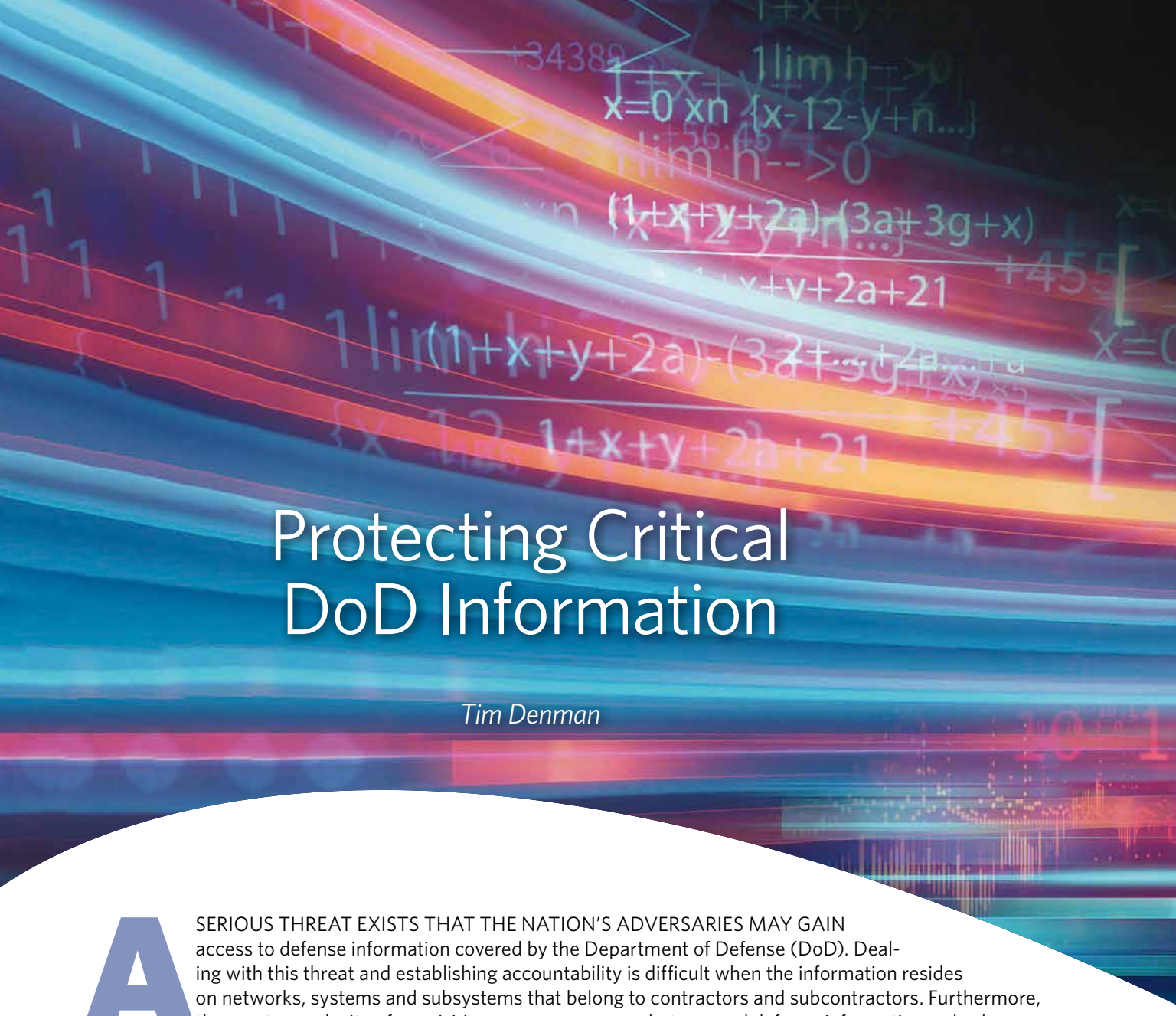

Protecting Critical DoD Information

Tim Denman

A SERIOUS THREAT EXISTS THAT THE NATION'S ADVERSARIES MAY GAIN access to defense information covered by the Department of Defense (DoD). Dealing with this threat and establishing accountability is difficult when the information resides on networks, systems and subsystems that belong to contractors and subcontractors. Furthermore, the great complexity of acquisition programs means that covered defense information—also known as DoD-controlled unclassified information (CUI)—is protected through contractual requirements to ensure protection throughout the program life cycle, from the earliest stages forward.

The DoD has taken several steps to safeguard information, and these steps encompass policy, training and enhanced communication. These steps include:

- **Developing Defense Federal Acquisition Regulation Supplement (DFARS)/leveraging Federal standards**—DFARS Clause 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*
- **Establishment of the Protecting Critical Technologies Task Force (PCTTF)**—Secretary of Defense Memorandum, October 2018
- **Town Halls, training and workshops**—collaborative effort between Defense Acquisition University (DAU), Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD[A&S]), Office of the Under Secretary of Defense for Research and Engineering (OUSD[R&E]), Office of the Department of Defense Chief Information Officer

Denman *since 2015 has been the Defense Acquisition University's Cybersecurity Learning Director and leads a geographically dispersed team. The team specializes in cybersecurity workshops and training.*

(ODoD CIO), Defense Contract Management Administration (DCMA), and NIST Manufacturing Extension Partnerships (MEP)—began in July 2018
- **Other initiatives**—including communication efforts, collaborative training efforts and ongoing partnerships

Developing DoD Policy, Leveraging Federal Policy

Covered defense information is unclassified controlled information or other information associated with the performance of a contract and requires safeguarding. Examples of this information include technical drawings, blueprints, plans, reports, computer software and documentation. DFARS Clause 252.204-7012 is required in all contracts except for those solely for the acquisition of commercial off-the-shelf items. This clause describes how covered defense information must be safeguarded and requires contractors and subcontractors to implement the security requirements included in NIST SP 800-171, Rev 1 (*Protecting CUI in Nonfederal Information Systems and Organizations*), when covered defense information is involved.

DFARs 252.204-7012 requires the program office/requiring activity to:

- Mark or otherwise identify in the contract, task order or delivery order covered defense information provided to the contractor by or on behalf of, DoD in support of the performance of the contract.

DFARs 252.204-7012 also requires the contractor/subcontractor to:

- Provide adequate security to safeguard covered defense information that resides on or is transiting through a contractor's internal information system or network.
- Report cyber incidents that affect a covered contractor information system or the covered defense information residing therein, or that affect the contractor's ability to perform requirements designated as operationally critical support.
- Submit malicious software discovered and isolated in connection with a reported cyber incident to the DoD Cyber Crime Center.
- Submit media/information as requested to support damage assessment activities.
- Flow down the clause in subcontracts for operationally critical support, or for which subcontract performance will involve covered defense information.

Establishment of the Protecting Critical Technologies Task Force

On Oct. 24, 2018, the Secretary of Defense established the Protecting Critical Technologies Task Force (PCTTF). His memo establishing this Task Force stated the following:

> I am committed to protecting the Department's critical technology. Each year, it is estimated that American industry loses more than $600 billion dollars to theft and expropriation. Far worse, the loss of classified and controlled unclassified information is putting the Department's investments at risk and eroding the lethality and survivability of our forces. Solving this problem will require an integrated effort across the Department. Because of the cross-cutting nature of the problem, I am establishing the Protecting Critical Technology Task Force (PCTTF).

This task force includes the Secretaries of the Military Departments; Chairman Joint Chiefs of Staff ; OUSD(R&E), OUSD(A&S); USD for Policy; USD for Intelligence; Director of Cost Assessment and Program Evaluation; DoD CIO; Commandant of the Marine Corps; Director, Defense Intelligence Agency; Director, Defense Security Service; U.S. Army Counter Intelligence; Naval Criminal Investigative Service; Air Force Office of Special Investigations; and any other representatives as deemed necessary by the Director.

While the statement above establishes a clear connection to the protection of covered defense information, the closing statement brings the importance of protecting DoD covered defense information into even greater focus. This statement reads:

> Working with our partners in the defense industry and research enterprise, we must ensure the integrity and security of our classified information, controlled unclassified information, and key data. The impacts of the loss of intellectual property and data cannot be overstated—we must move out to protect our resources and our forces.

Town Halls, Training and Workshops

For DoD acquisition policy to be effective, it must be understood and applied consistently across the military Services and the cross-departmental civilian Fourth Estate. Because of the criticality and time sensitivity of safeguarding covered defense information, DAU's role is especially important in training the acquisition workforce. In 2018, DAU Foundational Learning Directorate (FLD) Cybersecurity Professors Chris Newborn and Paul Shaw began meeting with industry and government agencies such as the NIST Manufacturing Extension Partnership (MEP) and the Defense Contract Management Agency to train the acquisition workforce and industry on the implementation of DFARS Clause 252.204-7012.

In July 2018, Office of the Secretary of Defense (OSD) representatives Vicki Michetti (Director of Cybersecurity Policy, Strategy, International Engagement, and the Defense Industrial Base [DIB] Cybersecurity Program, under the DoD Chief Information Officer); Melinda Reed (Program Protection Policy Lead, USD[R&E]); and Mary Thomas (Program Analyst for the Principal Director, Defense Pricing and Contracting [DPC], in the USD[A&S]), began co-presenting at DAU-sponsored Town Halls related to covered defense information and the DFARS clause listed above. Additionally, the three OSD representatives, in collaboration with DAU FLD Cybersecurity Professor Kim Kendall, developed a short series of videos discussing the principles of the DFARS clause 252.204-7012. These and related videos can be found on the DAU website at https://media.dau.edu/channel/CyberSecurity/62925431.

As of this writing, DAU and OSD have collaborated on five separate Town Hall events in four locations, ranging from San Diego, California, to Huntsville, Alabama, and trained more than 500 people on this important subject. Vicki, Melinda and Mary have been well received at each event and have answered many excellent questions generated by participants. In collaboration with OSD, DAU also has

led monthly covered-defense-information Town Halls and Workshops for more than 500 additional industry and acquisition workforce members at multiple locations during Fiscal Year (FY) 2019. Several follow-on events are scheduled through the end of FY 2019 and will continue into FY 2020.

Other Initiatives

DAU is forging a relationship with the DoD Cyber Crime Center (DC3), DoD-Defense Industrial Base (DIB) Collaborative Information Sharing Environment (DCISE), and is building a partnership with the Defense Security Service (DSS) Center for Development of Security Excellence. In addition, opportunities will be available to share and co-host courses, post training content on websites, and co-develop course curricula. Establishing a partnership with these DoD organizations that have unique subject-matter expertise will enable DAU to train the acquisition workforce required to protect covered defense information to support the warfighter and meet its mission.

DAU also plans to post a video on its website in the near future presented by Professor Chris Newborn on safeguarding covered defense information, and that video will cover education and training implementation discussion from a DAU Town Hall on the DoD and Industry protection of covered defense information. Newborn also began hosting a series of webinars in April, running through September 2019, addressing the challenges and sharing lessons learned related to implementing DFARS clause 252.204-7012. Finally, DAU continues to update its training across acquisition career fields to reflect the latest policies and guidance in cybersecurity and protecting covered defense information.

Summary

As stated by the Secretary of Defense, "The impacts of the loss of intellectual property and data cannot be overstated—we must move out to protect our resources and our forces." OSD, DAU, DCMA and many other organizations take this warning very seriously. Through DFARS clause 252.204-7012, the DoD is making great strides to protect covered defense information that resides on the DoD contractors' networks. An expansive communication, education and training effort is under way and the entire acquisition workforce must continue to be vigilant in this seemingly endless battle.

For more information on steps that DAU and other organizations are taking and if you would like a Town Hall or workshop in your area, please contact the author at the e-mail address below.

The author can be contacted at **tim.denman@dau.edu.**