What do intellectual property (IP) markings have to do with Department of Defense (DoD) acquisition? The short answer is: a lot. Consider all the noncommercial technical data and computer software (henceforth, these terms are called “data”) the DoD acquires—one weapon system alone could have thousands of detailed drawings, millions of software lines of code, and hundreds of technical manuals. IP markings on even a portion of that data could restrict the DoD’s use of the data, and its options for maintenance, sustainment and upgrades for the life of the weapon system. If the DoD is limited to the Original Equipment Manufacturer (OEM) for all product support, the OEM has a great advantage as a sole-source provider in setting the cost and schedule when negotiating with the DoD.

Verification of IP markings sounds like an easy, straightforward process. But IP rights and IP markings (including trade secret law and copyright law), along with commercial companies’ zealous protection of their IP—their “life blood” for business and profit—complicate everything involved with IP assessment, collection and management. In addition, it is important that program offices have personnel sufficiently trained in IP issues, including identification of the proper IP markings and the adjudication process. Another challenge of verifying IP markings and addressing any errors involves the amount of resources required to perform these tasks. Manually checking every computer software line of code for the correct IP markings is too time consuming and is most efficiently and effectively done through a computer scan performed by knowledgeable and trained operators. Pursuing the adjudication process to ensure corrections on mismarked data likewise requires substantial resources.

This article focuses on the importance of verifying the IP markings on data that affects our weapons systems. It introduces a DoD organization—the Joint Tactical Network Center (JTNC)—that performs IP marking verification as one step in its process. It also describes how improper IP markings adversely affect today’s warfighter and weapons systems. This article does not address IP markings for commercial data or Small Business Innovation Research Data. In addition, the contents of this article concern only contracts based on the Federal Acquisition Regulation.

Who Assigns IP Markings; What Are Improper IP Markings?

Contractors may place certain markings on data delivered to the government during the performance of a contract, but the markings must be identical to the language set out in the Defense Federal Acquisition
Regulation Supplement (DFARS) clauses. The DFARS is very specific on this point and even includes the exact wording that must be used in the markings, also known as legends. The appropriate markings depend on the rights the government has in the data delivered by the contractor under the contract. In order to restrict the government’s rights, the contractor generally must first inform the government, prior to contract award, of any restrictions by identifying them in an assertion list table provided with a proposal and then attached to the contract. The contractor must mark the delivered data in accordance with the assertion.

This assertion list table is required to identify the exact data to be delivered subject to any restrictions—either Limited Rights, Restricted Rights, Government Purpose Rights, or Specifically Negotiated License Rights. Data not listed in the assertion list table typically is treated as being provided with Unlimited Rights, and the contractor is not allowed to include any restrictive IP markings. Table 1 provides an example of a hypothetical assertion list table completed by the contractor. In this example, HI Robotics Document No. 123-4433 will be marked with a Government Purpose Rights legend with the exact wording as stated in the DFARS.

There are two types of improper IP markings—nonconforming and unjustified. Examples of each improper marking are listed in Table 2. Each type of improper marking requires its own resolution process or “adjudication” between the DoD and the contractor and/or subcontractor.

The Importance of IP Markings

One of the DoD’s core principles is to respect and protect privately developed IP, because IP is a valuable form of intangible property that is critical to the financial strength of businesses. The government should not remove IP markings or legends without following the required DFARS procedures.

IP Marking Verification—A Must Do

IP is one of the most difficult topics within the DoD acquisition community, involving complicated laws, policies, instructions and voluminous regulations. One of many major efforts the program office must undertake is the verification of IP markings on all delivered data. At a minimum, program offices should complete all of the following:

- Determine the data needs for the operation and sustainment of the weapon system
- Order the data by the inclusion of the Contract Data Requirement Lists (CDRL) in the contract
- Ensure that the contract conveys the necessary IP rights and ensure that all data is delivered to the program office

Without verifying all the IP markings on both printed documents and electronic files prior to the formal acceptance of the data, all of this hard work and the taxpayer funds invested are put in jeopardy.

There have been many instances where a contractor has delivered data that the government should be able to use without restriction (Unlimited Rights) while at the same time marking the data with “proprietary” or other restrictive markings. Contractors also have delivered noncommercial computer software source code to the DoD with a legend of Government Purpose Rights on the compact disc (CD), but when the government sought to use the software source code, the legend in the source code was “Restricted Rights.” With the “Restricted Rights” IP legend in the computer source code, no other company could modify or update this computer source code, even though the delivered CD was marked Government Purpose Rights. Other examples include:
• A contractor marked a final report with Limited Rights, despite government funding. After more than 2 years of negotiations, a formal challenge and a 90-day wait for the contractor to respond, the contractor conceded to the government’s position that its restrictive markings lacked any basis. The government’s use of the data was inappropriately restricted for about 3 years.

• The OEM delivered a satellite user’s manual with Unlimited Rights. The government prepared to release the manual as part of a future competition. However, the OEM stated the manual has “proprietary” elements notwithstanding the Unlimited Rights requirement. The issue is under review.

• The advanced electronic warfare system is a critical system element on an existing aircraft platform. The contract required the contractor to perform work on the system and deliver noncommercial technical data subject to Unlimited Rights (thus no IP markings/legends). The contractor and subcontractor provided the technical data but with nonconforming markings. The contracting officer rejected the deliverables and issued a final decision finding that the markings were nonconforming and directing the contractor to remove them. The contractor appealed the contracting officer’s final decision and requested a summary judgment from the Armed Services Board of Contract Appeals. In denying the summary judgment, the board found that the markings were nonconforming.

What is the moral of these stories? Verification of IP markings and enforcement of the government’s rights are vital to the development, sustainment and advancement of our wartime systems.
IP Markings Verification in DoD

This is where the JTNC comes in. The JTNC’s DoD Waveform Information Repository (IR) is chartered to verify all IP markings on data related to DoD radio waveforms. The IR protects and distributes documents and source code based on legal agreements or contracts between government and software developers.

The DoD Waveform IR provides IP marking verification services as an integral part of the process for software reuse on tactical radios. Program offices working with the IR anticipate that the IR will inspect and review the data and software that they supply to the IR. The IR uses automated tools to locate IP markings on thousands of files and ensure that the government complies with any restrictions.

Today’s tactical radios contain powerful processing capabilities conceived for broader use than older hardwired radio sets, and these radios are designed and configured with software applications as depicted in the photo collage below. The software can be reused in different software-defined radios. By ensuring that the IP markings are justified and conforming, the JTNC executes its mission of fostering the reuse of radio waveform software.

The DoD Waveform IR ensures that the data is ready for redistribution, including conducting IP marking verification activities, to support equitable, fair and competitive acquisition. The IR also performs more in-depth evaluations on waveforms IP license rights, software documentation, source code quality, and portability. When the JTNC takes custody of a software-defined waveform, the IP markings on the data delivered are verified before being reused. This happens before redistribution to support competitive acquisition or independent research and development by industry.

IP Markings on Noncommercial Technical Data

Figure 1 provides a notional graphical process to verify IP markings on data using the assertion list table. The timeline for this review is after the contract is awarded and prior to the contracting officer/contracting officer representative formally accepting the data via Department of Defense (DD) Form 250 (Material Inspection and Receiving Report). This review is conducted in two distinct ways: (a) all images or drawings are manually reviewed for IP markings, and (b) all other data is scanned by software for IP markings. Revisions to the manual review are under way to automate this process.

Images received individually or embedded within other
documents are manually reviewed for IP markings. Any markings found are compared against the assertion list table attached to the contract for possible nonconforming and/or unjustified IP markings. After the manual review, any nonconforming or unjustified IP markings are listed in a formal memo to the contracting officer and the JTNC’s legal counsel for resolution or adjudication.

An electronic review is in place to verify the IP markings on data that are not drawings (Software Requirements Specification, Software Test Plan, Interface Design Description, Software Development Plan, Software User’s Manual, Software Version Description, etc.). Both the IP Scan and SiMX software tools are custom built and tailored after each use to continuously improve and enhance results and minimize false positive findings. As with the manual review, any nonconforming or unjustified IP markings identified are listed in a formal memo to the contracting officer and the JTNC’s legal counsel for resolution or adjudication.

**Markings on Noncommercial Computer Software**

Figure 2 depicts a notional process to verify IP markings on noncommercial computer software. A government off-the-shelf scanning tool, IP scan, is used to verify IP markings in the source code of noncommercial computer software. The automated tool produces an HTML (Hyper Text Markup Language) scan report, listing the IP markings present in the computer source code file. The IP markings found in the scan report are manually reviewed and compared to the rights category identified in the assertion list table. The operator uses the scan report to check the computer software files and pinpoint unjustified or nonconforming markings. After the review, any nonconforming or unjustified IP markings are listed in a formal memo to the contracting officer and the JTNC’s legal counsel for resolution or adjudication.

**What Lies Ahead?**

JTNC leaders are continually advancing their development of tools and seeking better ways to accomplish the mission. They are integrating Optical Character Recognition technology to find markings on image file formats and eliminate the manual workload of spotting markings in large drawings and images. JTNC is engaged with the Defense Acquisition University (DAU) for training and workshops in the area of IP and IP markings. The JTNC and DAU will work hand in hand to continue to improve results in this important acquisition area.

Program offices can succeed in requiring contractors to deliver weapon systems data with the proper IP markings. Using the contractor’s assertions, with a little help from technology, an IP marking review can ensure that the best laid plans of the program office come to fruition, while respecting contractors’ valuable IP rights. By training your team regarding IP, IP markings and the process to review IP markings, you can enable this success.

The JTNC provides a markings verification service as an integral part of the process for reuse, and ensuring that data has the appropriate IP markings for reuse and redistribution. For more information about the JTNC’s markings verification capability, please contact the JTNC’s DoD Waveform Information Repository via email at dodir@navy.mil.

---

*Harris is a professor of Program Management at Defense Acquisition University in San Diego, California. He has more than 20 years of experience in defense acquisition and has a master of science degree in Systems Engineering from Johns Hopkins University and a master’s in Business from the Florida Institute of*
Technology. Cruz is with Joint Tactical Networking Center also in San Diego. She has more than 20 years of activity duty Air Force and Civil Service work and is experienced in human resources, technical systems requirements, and configuration management. Frank is a computer engineer in San Diego with 30 years’ experience in software development and operations, information assurance and radio frequency communications. He has a bachelor’s science degree in Electrical Engineering from the University of Kansas.

The authors can be contacted at howard.harris@dau.mil and david.frank@navy.mil.