

**Executive Summary:**

- Require that all systems purpose-built for DoD should have their source code available to the Department
- DoD should have the rights to and be able to modify the code when new conditions and features arise

**Full Recommendation 8:**

**Proposal:** Require that all systems purpose-built for the DoD should have their source code available to DoD. The Department should have the rights to and be able to modify the code.

**Comment:** A large number of modern defense systems are built and maintained in a manner that leaves control of the source code that runs the systems in the hands of industry. In some cases, changes to the code to adapt to new conditions, incorporate new features, or eliminate flaws require that contractors who control the code make the changes. This often incurs significant delays and costs. To enable more rapid innovation and customization that is required for modern defense operations, the DoD should have access to code running on its major purpose-built systems and to be able to make changes to that code. An additional benefit is the ability to reuse software in other parts of DoD.

The Department will honor existing contracts where DoD does not currently have access to the code, though modifying them if possible would be welcome. New contracts and systems should incorporate this recommendation, though, as with most major DoD policies, waivers and exemptions should be made available. This change should not prevent DoD from purchasing Software as a Service (SaaS) products that are open-source and would otherwise be ineligible for purchase due to contractual restrictions.

**Background:** As weapons and other systems become primarily software-driven platforms, and consistent with modern understanding of software systems as organic, evolving and improving, the Board places a very high premium on the native ability to rapidly fix and improve codes in delivered systems. DoD must have the ownership and capability to do so.

The Board recognizes three important challenges that must be addressed in this view of the world: First, DoD must have the necessary capability and capacity to understand, modify, verify, and validate code. Recommendations 2 and 9 speak to this issue. Second, transfer of risks and rewards must be managed. Clear requirements for what comprises delivery of major systems must protect the department from inheriting less than adequate original code that it will then have to maintain. Conversely, new business models will be required if systems providers do not have the financial returns that come from support of deployed systems. And, third, care must be taken to ensure IP rights are properly valued and protected.