Primary Recommendation D2
Security Considerations

Line of Effort	Change the practice of how software is procured and developed.
Recommendation	**Make security a first-order consideration for all software-intensive systems, recognizing that security-at-the-perimeter is not enough.**
Stakeholders	USD(A&S), CIO, DDS, SAE, DDR&E(AC), DOT&E
Background	Current DoD systems often rely on security-at-the-perimeter as a means of protecting code for unauthorized access. If this perimeter is breached, then a large array of systems can be compromised. Multiple GAO, DoDIG, and other reports have identified cybersecurity as a major issue in acquisition programs.
Desired State	DoD systems use a zero-trust security model in which it is not assumed that anyone who can gain access to a given network or system should have access to anything within that system. Regular and automated penetration testing is used to track down vulnerabilities, and red teams are engaged to attempt to breach our systems before our adversaries do.
Role of Congress	Review (classified) reporting of vulnerabilities identified in DoD systems and provide the resources required to ensure that hardware and operating systems are at current levels (see Recommendation B7, Hardware as a Consumable).

	Draft Implementation Plan	**Lead Stakeholders**	**Target Date**
D2.1	Adopt standards for secure software development and testing that use a zero-trust security model.	CIO, with DDS	Q3 FY19
D2.2	Develop, deploy, and require the use of IA-accredited (commercial) development tools for DoD software development.	CIO, PEO Digital	Q4 FY19
D2.3	Establish automated and red-team based penetration testing as part of OT&E evaluation (integrated with program development).	DOT&E	Q1 FY20
D2.4	Establish a red team responsible for ongoing vulnerability testing against any defense software system.	CIO with DDS	Q2 FY20
D2.5	Establish security as part of the selection criteria for software programs.	A&S with CIO, SAEs	Q3 FY20

SWAP concept paper recommendations related to this recommendation

10C	Only run operating systems that are receiving (and utilizing) regular security updates for newly discovered security vulnerabilities.
10C	Data should always be encrypted unless it is part of an active computation.
D&D	Create automated test environments to enable continuous (and secure) integration and deployment to shift testing and security left.

SWAP working group inputs (reflected in Appendix F) related to this recommendation

Sec	People must learn to appreciate that speed helps increase security. Security is improved when

	changes and updates can be made quickly to an application. Using automation, software can be reviewed quickly.
Sec	The AO must also be able to review documentation and make a risk decision quickly and make that decision on the process and not the product.
T&E	Establish a statutory “Live Fire” requirement on software-intensive systems as there is on “Covered Systems” for protecting our warfighters from kinetic threats. “Shoot at it” before design is complete and certainly before it is put into the operational environment.
T&E	Establish a federation of state-of-the-art cyber testing capabilities from non-profit institutions to support trusted, survivable, and resilient defense systems and ensure the security of software and hardware developed, acquired, maintained, and used by the DoD.
T&E	Establish cybersecurity as the “4th leg” in measurement of Acquisition system/program performance: Cost, Schedule, Performance, Cybersecurity.
T&E	Develop mechanisms to enforce existing software and cybersecurity policies (from cradle-to-grave) that are not (now) being adequately enforced.
T&E	Ensure each DoD Component is responsible for representing its own forces and capabilities in a digital modeling environment (e.g., M&S and digital twin), making them available to all other DoD users, subject to a pre-defined architecture and supporting standards. DIA will represent threat forces and capabilities in a digital form consistent with this architecture/standards. Programs are required to use DIA-supplied threat models, unless sufficient justification is provided to use other.

Related recommendations from previous studies

DSB09	In the Services and agencies, the CIOs should also have strong authorities and responsibilities for system certification, compliance, applications development, and innovation.
DSB09	The DOD CIO, supported by CIOs in the Services and agencies, should be responsible for certifying that systems and capabilities added to the enterprise do not introduce avoidable vulnerabilities that can be exploited by adversaries.
Sec809	Rec. 77: Require role-based planning to prevent unnecessary application of security clearance and investigation requirements to contracts.