RESEARCH SUMMARY

Enhancing Cybersecurity and Cyber Resiliency of Weapon Systems

Expanded Roles Across a System's Life Cycle

DON SNYDER, CHAD HEITZENRATER

To access the full report, visit www.rand.org/t/rrA1506-2

ISSUE

Weapon systems must be secure in a cyber contested environment, or they will not be able to carry out the missions that they are designed to support. How can engineering managed by program offices enhance the cybersecurity and cyber resiliency of weapon systems?

APPROACH

We surveyed current policy, relevant academic literature, and commercial practice and used our personal assessments of cybersecurity and cyber resiliency efforts in the Department of the Air Force (DAF) to identify gaps in the use of engineering for cybersecurity and cyber resiliency throughout the life cycle of weapon systems and to propose mitigations.

KEY FINDINGS

During the design phase, systems security engineering has recently become the policy within the Department of Defense (DoD) for cybersecurity and cyber resiliency of weapon systems, but it has not yet become the general practice in the DAF, and little policy or guidance directs specifically how to do it at the service level. An overreliance is still placed on the Risk Management Framework (RMF), which is largely carried out after systems engineering.

During the operations and sustainment phase, wing-level organizations perform much of the day-to-day security monitoring of weapon systems. However,

- They are not provided with authorized tools tailored to their weapon systems.
- The tools that they have cannot comprehensively monitor or defend their weapon systems.
- They are not provided with technical orders for what to do.
- Policy does not generally require feedback to the program offices of weapon system cyber status or cyber incidents.

continued

Cybersecurity and cyber resiliency are not central parts of current sustaining engineering or life cycle sustainment plans.

RECOMMENDATIONS

Our principal message can be summarized as a recommendation to develop and maintain an integrated engineering-based plan for the cybersecurity and cyber resiliency of each weapon system throughout its life cycle. For the design phase, we advocate that systems security engineering be enhanced by placing into the program plan and contract language:

- standards for designing systems with adequate cyber separability
- methods that the DoD will use to assess cyber resiliency of designs.

These engineering and contract statements need to be specific and measurable with regard to the security outcomes. Before these can be issued, further development and refinement, based on experience, is needed for both the standards and methods.

For the operations and sustainment phase, we advocate for increased use of sustaining engineering and the life cycle sustainment plans for cybersecurity and cyber resiliency. We recommend that program offices do the following:

- Equip wing-level organizations with approved tools for any cyber monitoring of a weapon system that are
  - catered to the weapon system
  - rigorously designed, developed, and tested with a security mindset, so as not to introduce attack vectors into the system
  - comprehensive in their ability to access the weapon system.
- Provide wing-level organizations, such as mission defense teams, with technical orders for the cyber monitoring of weapon systems.
- Receive information regarding any non-nominal behavior within the system boundary or cyber incident.
- Direct and approve any configuration change within the system boundary.

We recommend that the DAF develop an ecosystem for cyber sustaining engineering that uses or mirrors the ecosystem for aircraft maintenance, including processes such as Form 22 notifications for discrepancies in the above-mentioned technical orders and 107 requests for additional, cyber-related technical assistance from program offices.

Life cycle management plans should explicitly outline how the cybersecurity and cyber resiliency of each weapon system will be assured during operations, sustainment, and disposal.

Security should not be considered an activity implemented by RMF but one created by sound engineering and continuous vigilance, rigorously and continuously assessed by RMF.

RAND PROJECT AIR FORCE

RAND Project AIR FORCE (PAF), a division of RAND, is the Department of the Air Force's (DAF's) federally funded research and development center for studies and analyses, supporting both the United States Air Force and the United States Space Force. PAF provides the DAF with independent analyses of policy alternatives affecting the development, employment, combat readiness, and support of current and future air, space, and cyber forces. For more information, visit PAF's website at www.rand.org/paf.