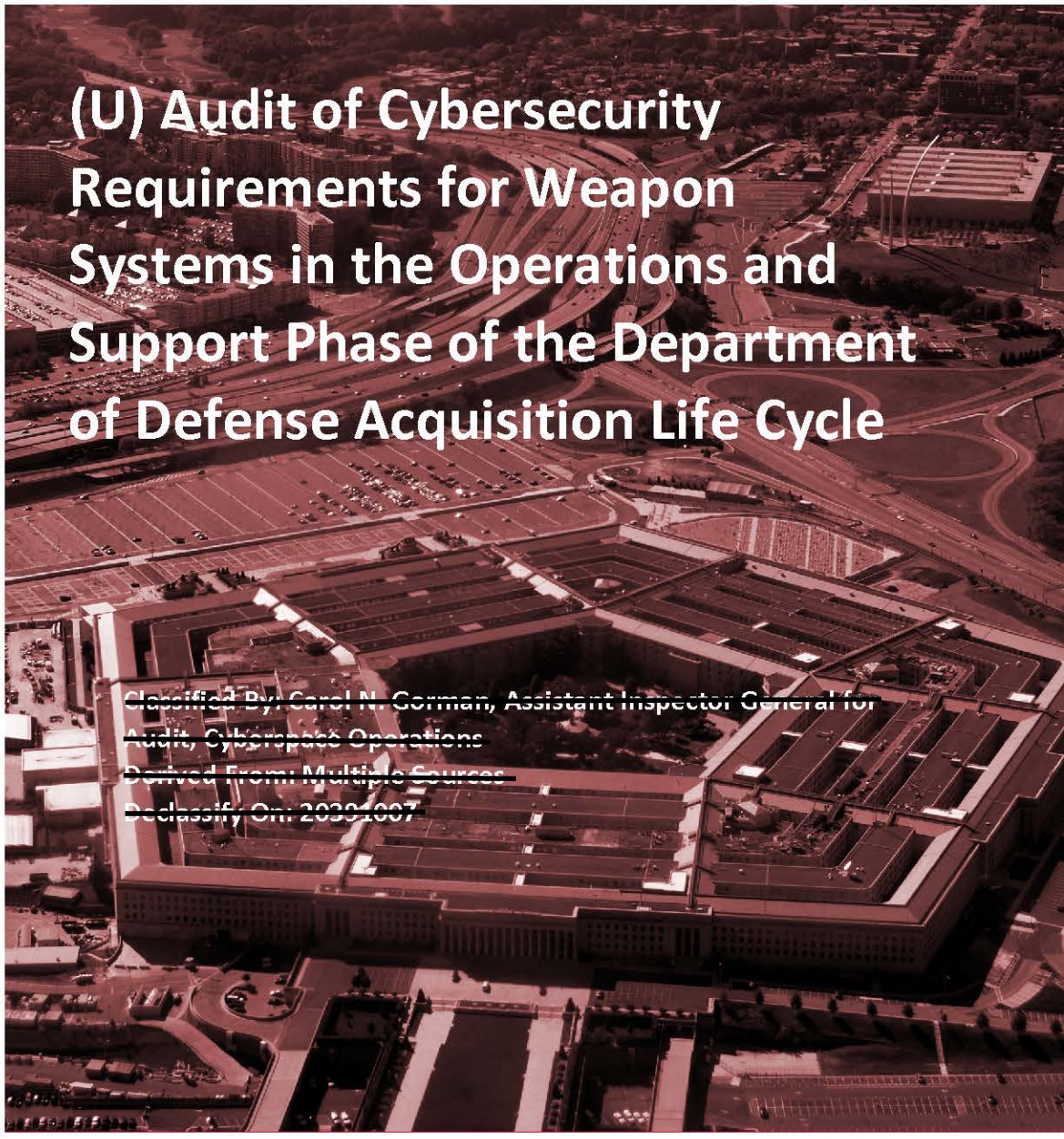
Report No. DODIG-2021-051

INSPECTOR GENERAL

U.S. Department of Defense

February 10, 2021



(U) Audit of Cybersecurity Requirements for Weapon Systems in the Operations and Support Phase of the Department of Defense Acquisition Life Cycle

~~Classified By: Carol N. Gorman, Assistant Inspector General for Audit, Cyberspace Operations~~
~~Derived From: Multiple Sources~~
~~Declassify On: 20391007~~

INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

~~SECRET//NOFORN~~

(U) Results in Brief

(U) Audit of Cybersecurity Requirements for Weapon Systems in the Operations and Support Phase of the Department of Defense Acquisition Life Cycle

(U) February 10, 2021

(U) Objective

(U) The objective of this audit was to determine whether DoD Components took action to update cybersecurity requirements for weapon systems in the Operations and Support (O&S) phase of the acquisition life cycle, based on publicly acknowledged or known cybersecurity threats and intelligence-based cybersecurity threats.

(U) Background

(U) A weapon system is a combination of one or more weapons with related equipment, materials, services, and personnel, and with means of delivery and deployment. The threats to weapon systems include equipment failure, environmental disruptions, human or machine errors, and purposeful attacks, such as cyber attacks. When successful, attacks on weapon systems can result in the loss of the confidentiality, integrity, and availability of information processed, stored, and transmitted by those systems.

(U) The DoD acquisition life cycle consists of five phases—Materiel Solution Analysis, Technology Maturation and Risk Reduction, Engineering and Manufacturing Development, Production and Deployment, and O&S. The O&S phase focuses on the cost-effectiveness of the support functions that sustain the system and the disposal of the system when it reaches the end of its life. The acquisition process also requires DoD Components to comply with the DoD Risk Management Framework (RMF) to improve cybersecurity and mitigate cybersecurity risks throughout the acquisition life cycle. The Risk Management Framework requires an authorization to operate for systems that receive, process, store, display, or transmit DoD information (unclassified and classified).

(U) Finding

(U) Program officials for the five DoD weapon systems that we assessed complied with Risk Management Framework requirements and obtained an authorization to operate. The officials also took actions to update cybersecurity requirements during the O&S phase of the acquisition life cycle based on publicly acknowledged or known cybersecurity threats and intelligence-based cybersecurity threats. Specifically, officials from the Army, Navy, Air Force, and U.S. Special Operations Command regularly obtained and analyzed cyber threats from various intelligence agencies to assess potential operational impacts to the weapon systems, and, based on their analysis, updated cybersecurity requirements to account for additional countermeasures implemented or needed to protect the weapon systems from the identified threats.

(U) We identified best practices employed by program officials that ensured that information gathered and analysis performed was sufficient to identify and mitigate potential malicious activity, cyber vulnerabilities, and threats; and assess the effectiveness of protection measures within the weapon system for data and cyber resiliency. For example, the program officials formed intelligence-based working groups, conducted cyber tabletop exercises, and regularly completed cyber threat and risk assessments to mitigate the DoD's susceptibility to cybersecurity threats to weapon systems.

(U) Because the O&S phase of the acquisition life cycle may last for years, DoD Components must continue to emphasize the protection of weapon systems by mitigating cyber threats throughout the O&S phase. For example, the B-2 Spirit Bomber, one of the weapon systems that we assessed, has been in the O&S phase for 16 years. Program officials for all weapon systems should consider the best practices described in this report when developing plans and procedures for reducing cybersecurity risks within their programs.

(U) Results in Brief

(U) Audit of Cybersecurity Requirements for Weapon Systems in the Operations and Support Phase of the Department of Defense Acquisition Life Cycle

(U) Recommendations

(U) We did not make any recommendations in this report

(U) Management Comments

(U) We did not make recommendations; therefore, no management comments are required.

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

February 10, 2021

MEMORANDUM FOR CHIEF MANAGEMENT OFFICER OF THE DEPARTMENT OF DEFENSE
SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING
UNDER SECRETARY OF DEFENSE FOR ACQUISITION AND SUSTAINMENT
COMMANDER, U.S. CYBER COMMAND
CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF DEFENSE

SUBJECT: (U) Audit of Cybersecurity Requirements for Weapon Systems in the Operations and Support Phase of the Department of Defense Acquisition Life Cycle (Project No. DODIG-2021-051)

(U) This final report provides the results of the DoD Office of Inspector General's audit. We considered management's comments on a discussion draft copy of this report when preparing this final report. We did not make any recommendations; therefore, no management comments are required.

(U) We appreciate the cooperation and assistance received during the audit. If you have any questions, please contact Carol Gorman at [redacted].

Carol N. Gorman
Assistant Inspector General for Audit
Cyberspace Operations

(U) Contents

(U) Introduction

(U) Objective

(U) The objective of this audit was to determine whether DoD Components took action to update cybersecurity requirements for weapon systems in the Operations and Support (O&S) phase of the acquisition life cycle, based on publicly acknowledged or known cybersecurity threats and intelligence-based cybersecurity threats. See the Appendix for a discussion of the scope, methodology, and prior coverage. See the Glossary for definitions of terms used in the report that relate to cybersecurity and weapon systems.

(U) Background

(U) A weapon system is a combination of one or more weapons with related equipment, materials, services, and personnel, and with means of delivery and deployment.[1] The threats to weapon systems include equipment failure, environmental disruptions, human or machine errors, and purposeful attacks, such as cyber attacks. When successful, attacks on weapon systems can result in the loss of the confidentiality, integrity, and availability of information processed, stored, and transmitted by those systems.

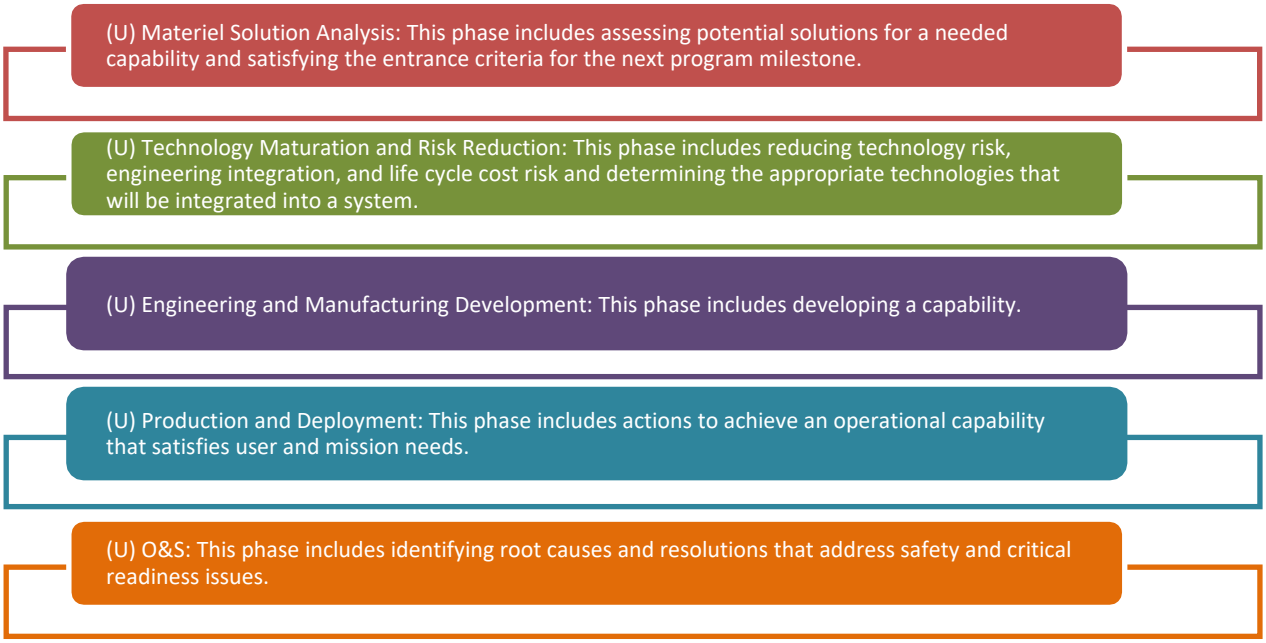
(U) Department of Defense Acquisition Life Cycle Phases

(U) DoD Instruction (DoDI) 5000.02T defines the DoD acquisition life cycle for DoD acquisition and weapon systems acquisition programs. According to the Instruction, the DoD acquisition life cycle consists of five phases—Materiel Solution Analysis, Technology Maturation and Risk Reduction, Engineering and Manufacturing Development, Production and Deployment, and O&S.[2] This audit focused on weapon systems in the O&S phase of the acquisition life cycle. The O&S phase focuses on the cost-effectiveness of the support functions that sustain the system and the disposal of the system when it reaches the end of its life. Figure 1 briefly describes each phase of the DoD acquisition life cycle.

[1] (U) Office of the Chairman of the Joint Chiefs of Staff, "Department of Defense Dictionary of Military and Associated Terms," October 2019.

[2] (U) DoDI 5000.02T, "Operation of the Defense Acquisition System," January 7, 2015 (Incorporating Change 7, April 21, 2020), is transitional guidance that will eventually be canceled or transition to a new issuance as outlined within this Instruction.

(U) Figure 1. Department of Defense Acquisition Life Cycle Phases



(U) Source: The Department of Defense Office of Inspector General (DoD OIG).

(U) DoDI 5000.02T also defines the responsibilities and procedures for implementing cybersecurity throughout all five phases. DoDI 5000.02T requires DoD Components to manage cybersecurity risks by implementing the Risk Management Framework (RMF).[3] The DoD began using the RMF in March 2014, as part of an overall Federal Government effort to improve cybersecurity and identify and mitigate cybersecurity risks throughout the acquisition life cycle.[4] The RMF is a six-step process that requires system owners to categorize the criticality and impact of loss of information and the loss of the system on the mission and the organization; select, implement, and assess security controls; examine the results of the controls assessed to determine whether an authorization to operate on the network should be issued; and continuously monitor implemented controls for changes and effectiveness. The authorization to operate is essential because it is an official management decision made about a system based on the risk accepted for the implemented security controls. The RMF requires an authorization to operate for systems that receive, process, store, display, or transmit DoD information (unclassified and classified).

[3] (U) Cybersecurity risk is the risk of financial loss, operational disruption, or damage to the weapon systems from the unauthorized access, use, disclosure, disruption, modification, or destruction of the system through cyberspace.

[4] (U) DoDI 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014, requires the DoD to implement the guidance within 3 years and 6 months, or implement the guidance before a system's re-authorization date or submit a request to deviate from the guidance to the Component's Chief Information Officer.

(U) DoDI 5000.02T requires program managers to implement cybersecurity standards to address specific program risks and determine the level of cyber protections needed for their programs.[5] Examples of cyber threat protection measures include safeguarding information and incorporating system protections for information security, operations security, and physical security. DoDI 5000.02T requires program managers to evaluate and mitigate cybersecurity risks by:

- (U) requesting cyber threat information and using threat assessments to identify the impact to operational systems;
- (U) protecting program and systems information, critical program information (CPI), and systems from adversary targeting; and
- (U) updating cybersecurity and related system security requirements, such as capability production documents, program protection plans (PPP), and test and evaluation master plans throughout the system's life cycle as cyber threats and systems evolve.[6]

(U) DoD Weapon System Programs Assessed

(U) We assessed five weapon system programs in the O&S phase of the acquisition life cycle. Specifically, we assessed one Army system, two Navy systems, one Air Force system, and one U.S. Special Operations Command system. The Table identifies the weapon systems included in the audit scope.

[5] (U) Program managers are designated individuals with responsibility to accomplish the program objectives for developing, producing, and sustaining acquisition programs that meet operational needs.

[6] (U) Capability production documents provide authoritative, testable capabilities to support the production, testing and deployment of a system. PPPs are continuously updated plans used by program managers to manage security risks to critical program information and mission-critical functions and components. Test and evaluation master plans provide a framework of developmental, operational, or live-fire activities for testing and evaluating system or network security.

(U) Table. Department of Defense Weapon Systems in the Audit Scope

(U) Weapon System	Weapon System Description	DoD Component
Advanced Threat Infrared Countermeasures/Common Missile Warning System (ATIRCM/CMWS)	Laser-based infrared countermeasure system that interfaces with the Common Missile Warning System, which is an integrated infrared countermeasure suite using ultraviolet sensors, to display threats and deploy countermeasures.	Army
Multifunctional Information Distribution System (MIDS)	Multiservice, wireless, and jam-resistant information system that provides communications that support air, ground, and maritime-based operations.	Navy
Advanced Anti-Radiation Guided Missile (AARGM)	Uses radar from multiple sources of information to track and target enemy air defense systems.	Navy
B-2 Spirit Bomber	A system of systems that work together to enable successful missions to deliver nuclear and conventional munitions.	Air Force
AC-130J Precision Strike Package (PSP)	Provides time-sensitive targeting and supports a key operational concept of precision engagement requirement.	U.S. Special Operations Command **(U)**

(U) Source: The DoD OIG.

(U) Review of Internal Controls

(U) DoDI 5010.40 requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls.[7] We did not identify any internal control weaknesses related to developing and updating cybersecurity requirements based on risk for the programs we assessed. We identified best practices for assessing risk and updating cybersecurity requirements for weapon system programs in the O&S phase of the acquisition life cycle, to mitigate cybersecurity threats. These best practices were conducting cyber threat and risk assessments, forming intelligence working groups, and conducting cyber tabletop exercises.

[7] (U) DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013.

(U) Finding

(U) Weapon System Program Officials Complied with the Risk Management Framework and Took Actions to Assess and Mitigate Risk in the Operations and Support Phase of the Acquisition Life Cycle

(U) Program officials for the five DoD weapon systems that we assessed complied with RMF requirements and obtained an authorization to operate. The officials also took actions to update cybersecurity requirements during the O&S phase of the acquisition life cycle based on publicly acknowledged or known cybersecurity threats and intelligence-based cybersecurity threats.[8] Specifically, officials from the Army, Navy, Air Force, and U.S. Special Operations Command regularly obtained and analyzed cyber threats from various intelligence agencies to assess potential operational impacts to the weapon systems, and, based on their analysis, updated cybersecurity requirements to account for additional countermeasures implemented or needed to mitigate identified threats to weapon systems.

(U) We identified best practices that program officials employed to ensure that the information gathered and analysis performed was sufficient to identify and mitigate potential malicious activity, cyber vulnerabilities, and threats; and to assess the effectiveness of the data and cyber resiliency protection measures within the weapon system. For example, some of the program officials formed intelligence-based working groups, conducted cyber tabletop exercises, and completed cyber threat and risk assessments to mitigate cybersecurity threats to the weapon systems.

(U) Because the O&S phase of the acquisition life cycle may last for years, DoD Components must continue to emphasize the protection of weapon systems by mitigating cyber threats throughout the O&S phase. For example, the B-2 Spirit Bomber, one of the weapon systems we assessed, has been in the O&S phase for over 16 years. Due to the system's age, it is continuously exposed to changing threat environments and new cybersecurity vulnerabilities. Program officials, for all weapon systems, should consider the best practices described in this report when developing plans and procedures for mitigating cybersecurity risks to weapon systems, especially officials with systems in the O&S phase of the acquisition life cycle.

[8] (U) For the purpose of this report, program officials include program managers, program executive officers, deputy program managers, information system security managers, information security officers, chief engineers, information technology leads, and information assurance leads.

(U) Actions Taken by Program Officials Mitigated Cybersecurity Risk Affecting Weapon Systems in the Operations and Support Phase

(U) Program officials for the five weapon systems that we reviewed complied with RMF requirements and took actions to assess risk, including actions such as forming intelligence working groups and conducting cyber tabletop exercises, updating cybersecurity requirements, and mitigating the impact that publicly acknowledged or known cybersecurity threats and intelligence-based threats could have on the survivability and resiliency of the weapon systems. DoDI 5000.02T requires program managers to manage risk to their programs throughout the programs' life cycles, including programs in the O&S phase, by identifying known risks; the probability of occurrence; the consequences of occurrence if not mitigated; and actions needed to mitigate those risks.

(U) To determine whether weapon system program officials took actions to update cybersecurity requirements for their programs, we analyzed documentation, such as capability production documents and PPPs, intelligence and cyber threat assessments, as well as cybersecurity penetration assessments. In addition, we identified risk management activities and countermeasures that the weapon system program officials implemented, tested, or identified as future system upgrades necessary to mitigate the cybersecurity threats. The following sections describe the actions program officials took to update the cybersecurity requirements and mitigate the threats for the five systems we assessed—the Advanced Threat Infrared Countermeasures/Common Missile Warning System (ATIRCM/CMWS), Multifunctional Information Distribution System (MIDS) Joint Tactical Radio System, Advanced Anti-Radiation Guided Missile (AARGM), B-2 Spirit Bomber (B-2 Spirit), AC-130J, and Precision Strike Package (AC- 130J PSP).

(U) Advanced Threat Infrared Countermeasures/Common Missile Warning System

(U) ATIRCM/CMWS program officials assessed cybersecurity risks and took actions to mitigate cybersecurity threats to the program. The ATIRCM/CMWS, which was originally designed in 1995 for use by the Army, Navy, and Air Force, is the Army's Aircraft Survivability Equipment used to protect aircrews from advanced threats from surface-to-air missiles.[9] The ATIRCM/CMWS exchanges information with the host aircraft but does not connect to an external network or the DoD Information Network. The CMWS identifies an inbound infrared missile or Man Portable Air Defense System

[9] (U) The Navy and Air Force withdrew from the ATIRCM/CMWS program in 2000. In October 2003, the Army funded the ATIRCM/CMWS to restore the program and began fielding it in November 2003.

(U) missile and sends an alert signal to the ATIRCM. Once the ATIRCM receives the missile alert signal, it uses an infrared tracker to more precisely locate the missile. The ATIRCM then fires a laser jammer (which contains jamming codes) designed to confuse the missile's guidance system. Figure 2 shows how the ATIRCM/CMWS operates.

(U) Figure 2. Operation of the Advanced Threat Infrared Countermeasures/Common Missile Warning System

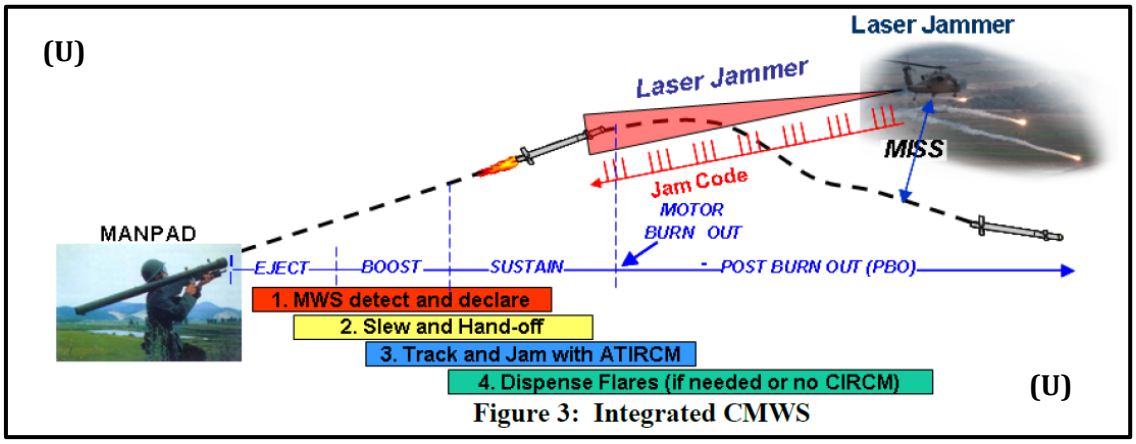


Figure 3: Integrated CMWS

(U) Source: CMWS Program Executive Office.

(U) The ATIRCM and CMWS Program entered the O&S phase of the acquisition life cycle in November 2009 and May 2006, respectively.[10] The ATIRCM/CMWS was in operation before the RMF was initiated, and was exempted from following a security framework until the ATIRCM/CMWS Program Management Office for Aircraft Survivability Equipment transitioned to the RMF and obtained an authorization to operate in 2019.

~~(S)~~ In addition to complying with RMF requirements and obtaining an authorization to operate, the ATIRCM/CMWS officials collaborated with contractors and the Intelligence Community to identify and assess the potential impact of cybersecurity threats, and to discuss methods to mitigate those threats. Based on the collaboration efforts, the mitigation methods identified, and the completed system assessments, the Program Management Office and Program Executive Office updated the PPP for managing ATIRCM/CMWS cybersecurity risks affecting program information and mission-critical functions and components in accordance with DoDI 5000.02T requirements. The Program Management Office also participated in monthly briefings with the [redacted] to identify relevant threats to the

[10] (U) The CMWS can function as a stand-alone system, but the ATIRCM cannot function alone. When the ATIRCM is installed with the CMWS, it improves the countermeasures dispenser's ability to defeat infrared guided missiles

~~(S)~~ ATIRCM/CMWS. Furthermore, the ATIRCM/CMWS Program Management Office developed and implemented an ongoing process to assess intelligence-based threats, updated the program's cybersecurity requirements, when warranted, and implemented countermeasures to address specific threats. For example, the ATIRCM/CMWS Program Management Office performed a series of tests to verify that the additional ATIRCM/CMWS countermeasures [redacted]. The ATIRCM/CMWS Program Management Office used the results of the tests to update cybersecurity requirements with the steps taken to address the specific threats. For example, [redacted].

(U) Multifunctional Information Distribution System

~~(S)~~ MIDS Joint Tactical Radio System officials assessed cybersecurity risks and took actions to mitigate cybersecurity threats to the program. The MIDS Joint Tactical Radio System enables communications between land, sea, and air forces through a Tactical Data Link to support joint operations and improve information sharing between geographically separated forces. The system uses [redacted] to maintain secure communications. Figure 3 shows a MIDS radio.

(U) Figure 3. Multifunctional Information Distribution System Joint Tactical Radio System

(U) Source: MIDS Program Management Office.

(U) In May 2003, the MIDS Program entered into the O&S phase of the acquisition life cycle. The MIDS was in operation before the RMF was initiated, and was exempted from following a security framework until the MIDS Program Manager began transitioning to the RMF in January 2016.

~~(U//FOUO)~~ MIDS is [redacted], which according to DoDI 8510.01, does not require the system owner to obtain an authorization to operate or continuously monitor security requirements.[11] However, the National Security Agency does require life-cycle change-management oversight, review, and approval of changes of the MIDS program. Platform information technology does not connect to the DoD Information Network directly; instead, it connects to a trusted host interface (also known as a receiving organization), such as an aircraft or a ship. The owner of the trusted host interface is responsible for assessing the impact of security risks associated with hosting MIDS on the owner's system or network. However, the MIDS Program Management Office is responsible for mitigating risks specific to MIDS identified by the trusted host interface owner.

~~(S)~~ In addition to complying with RMF requirements for platform information technology, the MIDS Program Management Office collaborated with the Intelligence Community to continuously assess cybersecurity threats. [redacted] the MIDS Program Management Office has obtained and used intelligence-based threat information from a threat working group to continuously assess risk based in part on the RMF process, and has updated cybersecurity requirements to mitigate the impact that known cybersecurity threats and intelligence-based threats have on the MIDS Joint Tactical Radio System.

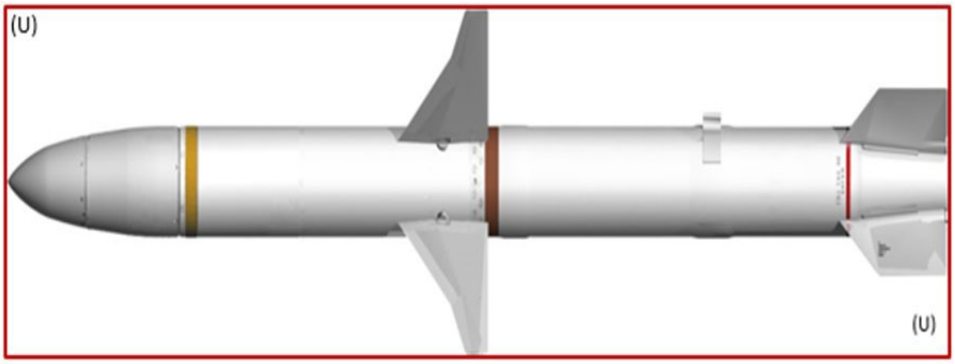
~~(S)~~ The working group, which includes members from agencies such as the [redacted], analyzed intelligence-based knowledge gaps of current threat capabilities related to the MIDS Joint Tactical Radio System. For example, when the MIDS Joint Tactical Radio System security architecture changed [redacted], the National Security Agency worked with the MIDS Program Office and revised the capability production documents to include details on system updates and newer capabilities, as well as intelligence-based threat information and the threat impacts. [redacted]. The MIDS Program Office used the analysis to update the capability production documents to highlight the changes needed and enhancements made to the MIDS terminals to mitigate the risk of this threat. The first of two system upgrades occurred in [redacted]. [redacted].

[11] (U) Platform information technology is essential to DoD missions and must complete the appropriate evaluation and configuration processes before integrating with or connecting to an information system.

(U) Advanced Anti-Radiation Guided Missile

~~(S//NF)~~ AARGM program officials assessed cybersecurity risks and took actions to mitigate cybersecurity threats to the program. The Navy designed the AARGM, which provides the [redacted]. Figure 4 shows the AARGM and its major components.

(U) Figure 4. Advanced Anti-Radiation Guided Missile



(U) Source: AARGM Direct and Time Sensitive Strike Program Office, PMA-242.

~~(S//NF)~~ In July 2012, the AARGM Program entered the O&S phase of the acquisition life cycle. Because the AARGM was in operation before the RMF was initiated, AARGM program officials followed a different security framework until the AARGM Program Executive Office transitioned to the RMF and obtained an authorization to operate in June 2018. In addition to complying with RMF requirements and obtaining an authorization to operate, the AARGM program officials used cyber risk and threat assessments provided by the Naval Criminal Investigative Service to assess risks and update requirements to mitigate cybersecurity risk. For example, [redacted]

(U) B-2 Spirit Bomber

~~(U//FOUO)~~ B-2 Spirit program officials assessed cybersecurity risks and took actions to mitigate cybersecurity threats to the program. [redacted]

~~(U//FOUO)~~ The B-2 Spirit is a long-range bomber that is capable of delivering both nuclear and conventional munitions. [redacted]. Figure 5 shows a B-2 Spirit in flight.

(U) Figure 5. B-2 Spirit

(U) Source: Barksdale Air Force Base.

~~(U//FOUO)~~ In December 2003, the B-2 Program entered the O&S phase of the acquisition life cycle. [redacted].[12]

~~(U//FOUO)~~ The B-2 Spirit Division updated cybersecurity requirements based on intelligence-based threat assessments and cyber resiliency penetration testing results. [redacted]

[12] (U) The B-2 Spirit transitioned to the Air Force Life Cycle Management Center and began using Air Force Instruction 17-101, "Risk Management Framework (RMF) For Air Force Information Technology (IT)," February 6, 2020, which aligns with DoDI 8510.01. The B-2 Spirit received an authorization to operate in July 2020 from the Air Force Life Cycle Management Center's Avionics Engineering Division. DoD Joint Special Access Program Implementation Guide, October 9, 2013, was canceled and replaced by the DoD Joint Special Access Program Implementation Guide, April 11, 2016.

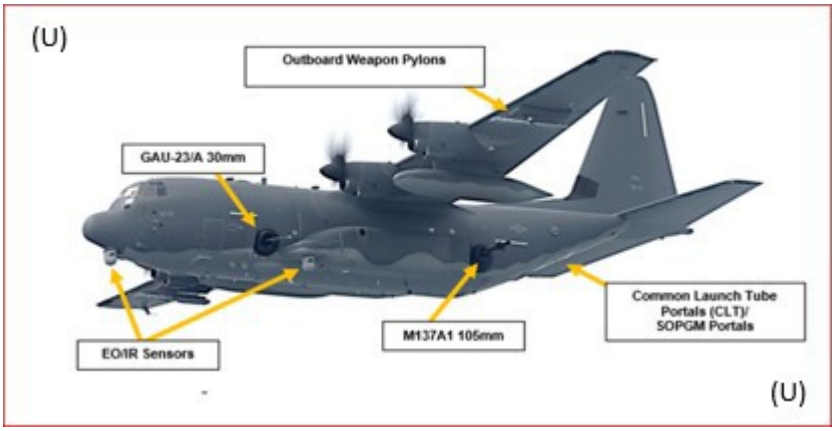
(U//FOUO) [redacted]. In addition, the B-2 Spirit Division updated the Cybersecurity Strategy, a B-2 Spirit requirements document, with details of the security improvements. [redacted].

~~(U//FOUO)~~ In addition, [redacted]. However, the B-2 Spirit Division information system security manager provided a memorandum stating that cyber testing was [redacted].

(U) AC-130J Precision Strike Package

~~(S)~~ AC-130J PSP officials assessed cybersecurity risks and took actions to mitigate cybersecurity threats to the program. [redacted]. Figure 6 shows the PSP external configuration on AC-130J.

(U) Figure 6. PSP External Configuration on AC-130J



(U) Source: AC-130J Program Office.

~~(S)~~ In September 2016, the AC-130J PSP Program entered the O&S phase of the acquisition life cycle through an aircraft modification process to support current and future combat operations. Because the PSP program was in operation before the RMF was initiated, the PSP program officials followed a different security framework until transitioning to the RMF in September 2017 and [redacted]. In addition to complying with RMF requirements and obtaining an authorization to operate, the PSP Program Executive Office implemented a process to mitigate cybersecurity risks. This process included meeting with applicable stakeholders to discuss cybersecurity issues identified in security and risk assessments, updating the program's cybersecurity requirements, and implementing countermeasures to mitigate specific threats.

~~(S)~~ In addition, the AC-130J PSP officials performed a series of assessments, which were used to develop Risk Assessment Reports, to identify and mitigate cybersecurity threats to the aircraft and subsystems that were designed to destroy specific targets. For example, a 2019 cyber risk assessment identified a cybersecurity threat [redacted], PSP program officials updated the PPP to describe the threats, vulnerabilities, and the specific countermeasures for improving the information and communications security of the PSP. [redacted].

(U) Best Practices for Reducing Cybersecurity Threats to DoD Weapon Systems

(U) Program officials for the five weapon systems that we assessed complied with the RMF or its equivalent and shared actions they took that we believe other program managers should use for mitigating cybersecurity threats to DoD weapon systems. Some examples of these best practices include the following.

- **(U) Conducting Cyber Threat and Risk Assessments.** Program officials regularly completed cyber threat and risk assessments to identify cybersecurity risks. Program officials worked with cyber working groups and applicable stakeholders to update the cybersecurity and system security-related requirements using the assessment results. For example, program officials for one weapon system worked with applicable stakeholders to identify a threat and used the results to update the PPP and implement specific countermeasures to mitigate the specific threat.

- **~~(S)~~ Forming or Participating in Intelligence-Based Working Groups.** Program officials formed intelligence-based working groups and collaborated with the Intelligence Community to assess current cybersecurity threats. Program officials in working groups used threat assessments to document the impact to operational systems. For example, program officials for one weapon system used intelligence [redacted].

- **(U) Conducting Cyber Tabletop Exercises.** Program officials for one weapon system conducted cyber table top exercises to identify potential attack vectors and assess the potential impacts of these attacks on the system to prioritize test activities. The results of the cyber tabletop exercise were used to identify the top mission areas tested during penetration testing.

(U) Conclusion

(U) The DoD continues to face increasingly sophisticated and changing cyber attacks by malicious actors, which necessitates processes and procedures to continually assess and mitigate cybersecurity risks to ensure that weapon systems perform when needed and as intended. Compromised weapon systems threaten the safety of DoD service members, adversely affect National Defense Strategy objectives, and reduce the United States' technical advantage against our adversaries. Regularly assessing cybersecurity risks, updating cybersecurity requirements, and taking actions to mitigate cybersecurity risks by implementing security controls and other countermeasures decreases the DoD's susceptibility to cybersecurity threats and

(U) ensure that the weapon systems operate as intended. Program officials should consider the best practices described in this report when developing plans and procedures for reducing cybersecurity risks to weapon systems, especially those in the O&S phase of the acquisition life cycle.

(U) Appendix

(U) Scope and Methodology

(U) We conducted this performance audit from April 2019 through December 2020 in accordance with generally accepted government auditing standards. However, due to the DoD's implementation of maximum telework during the coronavirus disease-2019 pandemic, the audit was suspended from March 24, 2020, through July 6, 2020. Generally accepted government auditing standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

(U) To determine the DoD's process for assessing cybersecurity of weapon systems, we interviewed officials from the offices of Director, Operational Test and Evaluation; Under Secretary of Defense for Acquisition and Sustainment; Under Secretary of Defense for Research and Engineering; DoD Chief Information Officer; Joint Chiefs of Staff, Command, Control, Communications, and Computers/Cyber Directorate; and Acquisition components for the Army, Navy, Air Force, U.S. Special Operations Command, and the Missile Defense Agency. In addition, we interviewed the Deputy Program Manager for the Defense Acquisition Management Information Retrieval (DAMIR) to determine the purpose, management, and security protocols in place for the DAMIR system. We also reviewed DoD and Component-level guidance to determine acquisition, cybersecurity, risk management, and program requirements specific to each weapon system reviewed.

(U) We received a list of weapon systems from DAMIR, the most recent from November 2019, and conducted a data call with DoD Components to obtain a list of weapon systems within their acquisition portfolio. We compared the list from DAMIR to the information provided separately by the DoD Components to verify whether both sources accounted for all weapon systems and to select the programs included in the audit scope. We nonstatistically selected five weapon systems for inclusion in the audit scope and verified that each program was in the O&S phase of the acquisition lifecycle.

- (U) ATIRCM/CMWS (Army)
- (U) MIDS (Navy)
- (U) AARGM (Navy)

- (U) B-2 Spirit Bomber (Air Force)
- (U) AC-130J PSP (U.S. Special Operations Command)

(U) After selecting the programs, we met with the program officials and analyzed documentation, such as the capability production documents, PPP, and test and evaluation master plans, to determine whether program officials continuously assessed risk throughout the O&S phase and, when necessary, updated cybersecurity requirements based on publicly acknowledged or known cybersecurity threats and intelligence-based cybersecurity threats. We also assessed actions taken by program officials to comply with the DoD RMF in relation to reducing cybersecurity risks affecting each weapon system.

(U) Use of Computer-Processed Data

(U) We used computer-processed data from DAMIR to nonstatistically select weapon systems for inclusion in the audit scope. The DoD acquisition community uses DAMIR to manage various data sources and to organize information for the Selected Acquisition Reports for Major Defense Acquisition Programs to meet congressional reporting requirements.[13]

(U) We also used lists of weapon systems obtained from the Army Acquisition Program Master List; the Navy Research, Development, and Acquisition Information System; and the Air Force Project Management Resource Tools.[14] We assessed the reliability of the data by comparing the lists of weapon systems from Army Acquisition Program Master List, Research, Development & Acquisition Information System, and Project Management Resource Tools to the data we obtained from DAMIR.
We determined that the data from DAMIR, Army Acquisition Program Master List; Navy Research, Development, and Acquisition Information System; and Air Force Project Management Resource Tools were sufficiently reliable for the purpose of selecting programs for this audit.

(U) Use of Technical Assistance

(U) We worked with the DoD OIG Quantitative Methods Division to develop a nonstatistical sampling methodology to select the weapon systems included in the audit scope.

[13] (U) The Selected Acquisition Reports are required to be delivered to Congress by section 2432, title 10, United States Code, "Selected Acquisition Reports," and include program-specific information, such as the mission of the program; costs; funding; procurement schedule; quantity of items to be purchased; and contracts.

[14] (U) The Army migrated from the Army Acquisition Program Master List to Project Management Resource Tools in December 2019. Due to their small number of acquisition programs, U.S. Special Operations Command did not use a system to generate program lists. U.S. Special Operations Command queried its Program Executive Offices to determine which programs were in the O&S phase.

(U) Prior Coverage

(U) During the last 5 years, the Government Accountability Office (GAO), the DoD OIG, and the Air Force Audit Agency issued four reports addressing cybersecurity challenges affecting weapon systems.

(U) Government Accountability Office

(U) Report No. GAO 19-439 "DoD Acquisition Reform – Leadership Attention Needed to Effectively Implement Changes to Acquisition Oversight," June 2019

> (U) The GAO determined that the DoD made progress in implementing reforms to restructure the oversight of Major Defense Acquisition Programs; however, questions remain on how some reforms will be carried out. The GAO also determined that the DoD faced implementation challenges, including disagreements about oversight roles and responsibilities. The GAO concluded that without developing a process for managing oversight roles and responsibilities, DoD officials were not well-positioned to assess whether reforms had the intended effects, such as improving innovation and delivering capability to the warfighter more quickly.

(U) Report No. GAO 19-128 "Weapon System Cybersecurity – DoD Just Beginning to Grapple with Scale of Vulnerabilities," October 2018

> (U) The GAO determined that the DoD routinely found mission-critical cyber vulnerabilities in systems that were under development. Although the GAO determined that the DoD was aware of limited vulnerabilities, it was not aware of the full range of threats. The GAO concluded that due to insufficient security controls, testers were able to take control of these systems, operate undetected, and in some cases, system operators were unable to effectively respond to the malicious activity.

(U) DoD OIG

(U) Report No. DODIG-2020-042, "Audit of the Service Acquisition Executives' Management of Defense Acquisition Category 2 and 3 Programs," December 20, 2019

> (U) The DoD OIG determined that Army, Navy, and Air Force Service Acquisition Executives did not appropriately identify or monitor whether their Departments' acquisition category 2 and 3 program costs and schedules aligned with their respective acquisition category designation. In addition, the DoD OIG determined that the Army's Program Executive Office for Combat Support and Combat Service Support did not inform or receive required approval from the Army Headquarters Data Administrator before deleting two

(U) programs from the Army's database used to track acquisition programs. As a result, the DoD OIG concluded that the Army, Navy, and Air Force could not accurately account for acquisition and program costs of up to $144 billion.

(U) Air Force Audit Agency

(U) Report No. F2018-0003-O1000, "Cybersecurity Program Management Configuration," December 22, 2017

(U) The Air Force Audit Agency determined that Air Force officials did not integrate cybersecurity into the design of weapon systems at Wright Patterson and Hanscom Air Force Bases. The Air Force Audit Agency concluded that system security was addressed through a set of activities and products that were not fully integrated, which created cybersecurity gaps in the programs.

(U) Source of Classified Information

(U) The documents listed below are sources used to support classified information within this report.

Source 1: (U) Capability Production Document for MIDS (Document is SECRET//NOFORN)
Declassification Date: October 7, 2039
Generated Date: October 7, 2017

Source 2: (U) Joint Requirements Oversight Council Memorandum for Evaluation of Cyber Vulnerabilities of Major Weapon Systems (Document is SECRET)
Declassification Date: March 20, 2039
Generated Date: May 25, 2016

Source 3: (U) Acquisition PPP for the PSP (Document is SECRET//NOFORN)
Declassification Date: October 25, 2038
Generated Date: January 13, 2014

Source 4: (U) Multidiscipline Counterintelligence Threat Assessment for AARGM (Document is SECRET//NOFORN)
Declassification Date: November 14, 2033
Generated Date: November 14, 2008

Source 5: (U) Cyber Risk Assessment for AARGM (Document is SECRET//NOFORN)
Declassification Date: June 27, 2048
Generated Date: June 27, 2019

Source 6: (U) ATIRCM/CMWS PPP (Document is SECRET//NOFORN)
Declassification Date: March 16, 2037
Generated Date: February 22, 2016

(U) Acronyms and Abbreviations

AARGM	Advanced Anti-Radiation Guided Missile
ATIRCM	Advanced Threat Infrared Countermeasures
CMWS	Common Missile Warning System
CPI	Critical Program Information
DAMIR	Defense Acquisition Management Information Retrieval
MIDS	Multifunctional Information Distribution System
O&S	Operations and Support Phase
PPP	Program Protection Plans
PSP	Precision Strike Package
RMF	Risk Management Framework

(U) Glossary

(U) Acquisition Program. A directed, funded effort that provides a new, improved, or continuing materiel, weapon, or information system, or a service capability in response to an approved need.

(U) Blue Team. A group responsible for defending an enterprise's use of information systems by maintaining its security posture against a group of attackers.

(U) Capability Production Document. This document provides authoritative, testable capabilities for the Production and Deployment Phase of an acquisition program. This document is also required to capture the information necessary to support the production, testing and deployment of a system and is also known as the Capability Development Document.

(U) Critical Program Information (CPI). A capability element that contributes to the warfighters' technical advantage, which if compromised, undermines U.S. preeminence.

(U) Cyber Attack. An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disruption, disabling, destroying, or maliciously controlling a computing environment or infrastructure; or destroying the integrity of the data or stealing controlled information.

(U) Cybersecurity Risk. The risk of financial loss, operational disruption, or damage from the failure of digital technologies used for informational or operational functions introduced to a system through electronic means from the unauthorized access, use, disclosure, disruption, modification, or destruction of a system.

(U) Cybersecurity Strategy. A required acquisition program document that details how a program will ensure that an information system can protect and defend itself from a cyber attack.

(U) Cybersecurity Threat. Anything that can exploit a vulnerability to harm a system, either intentionally or unintentionally.

(U) Cyber Vulnerability. A weakness in a system that could be exploited to gain access or otherwise affect the confidentiality, integrity, and availability of the system.

(U) Defense Acquisition Management Information Retrieval (DAMIR). A DoD system that provides enterprise visibility to acquisition program information needed by the acquisition community in managing Major Defense Acquisition Programs through web services, authoritative data sources, data collection, and data repository capabilities.

(U) DoD Information Network (DODIN). A global interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information.

(U) Jam/Jamming. A deliberate communication disruption meant to degrade the operational performance of a radio frequency.

(U) Malicious Actor. A participant (person or group) in an action or process that is characterized by malice or hostile action (intending harm) using computers, devices, systems, or networks.

(U) Man Portable Air Defense Systems (MANPAD). A shoulder fired surface to air anti-aircraft missile that can be carried and fired by a single individual or carried by several individuals and fired by more than one person acting as a crew.

(U) Network. Information systems implemented with a collection of interconnected components such as routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

(U) Program Protection Plan (PPP). A plan that should be continuously updated to manage the risks to CPI and mission-critical functions and components, as well as program and system information.

(U) Red Team. A group of people authorized and organized to emulate a potential adversary's attack.

(U) Resiliency. A system's ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises derived from actions in or through cyberspace.

(U) Survivability. The capability of a system or its crew to avoid or withstand a manmade hostile environment without impairing mission accomplishment.

(U) Tactical Data Link. A waveform that allows communication between land, sea, and air forces to support joint operations and improves information sharing between dispersed battle elements using data encryption and frequency hopping to maintain secure communications.

(U) Test and Evaluation Master Plan (TEMP). Documents the overall structure and objectives of the Test and Evaluation program. It provides a framework to generate detailed test and evaluation plans. It identifies the necessary developmental test and evaluation (DT&E), operational test and evaluation (OT&E), and live fire test and evaluation (LFT&E) activities. It relates program schedule, test management strategy

(U) and structure, and required resources to critical operational issues, critical technical parameters objectives and threshold documented in the capability development document, evaluation criteria, and milestone decision points.

(U) Weapon System. A combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment required for self-sufficiency.


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

Whistleblower Protection

U.S. Department of Defense

Whistleblower Protection safeguards DoD employees against retaliation for protected disclosures that expose possible waste, fraud, and abuse in government programs. For more information, please visit the Whistleblower webpage at http://www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whisteblower-Reprisal/ or contact the Whistleblower Protection Coordinator at Whistleblowerprotectioncoordinator@dodig.mil

For more information about DoD OIG reports or activities, please contact us:

Congressional Liaison
703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

DoD OIG Mailing Lists
www.dodig.mil/Mailing-Lists/

Twitter
www.twitter.com/DoD_IG

DoD Hotline
www.dodig.mil/hotline

~~SECRET//NORFORN~~

DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, Virginia 22350-1500
www.dodig.mil
DoD Hotline 1.800.424.9098

~~SECRET//NOFORN~~