CH 7–1. Purpose

This chapter provides guidance to acquisition personnel on how to acquire, integrate, manage, and use intelligence information to deliver maximum warfighting capability at minimum risk to cost, schedule, and performance. It provides a reference guide of exemplars, best practices, and resources for intelligence support to Department of Defense (DoD) acquisition processes.

CH 7–2. Background

Modern technologies are often highly dependent upon a variety of scientific and technical intelligence products throughout every stage of the research and development lifecycle. This, combined with a rapidly advancing adversary who is challenging the delivery of United States (US) warfighting capabilities, drives great importance to effective use and integration of intelligence within acquisition processes. When sufficiently integrated, intelligence can ensure that capability requirements are realistic, that they are translatable into engineering specifications that can compete in the future operational environment, and that the Nation’s best possible threat representations assist in ensuring what is designed will in fact meet war winning needs.

There are many examples to show that Program and Project Managers (PMs) who consider intelligence routinely, and effectively plan for future intelligence needs, deliver more capable and resilient systems than those who do not.

CH 7–3. Business Practice

Acquisition Intelligence is the program office function that identifies and manages intelligence dependencies for the acquisition effort and applies threat insights to guide design and development decisions. Each Service has a cadre of Acquisition Intelligence specialists with the tools, knowledge and means to leverage the full range of Defense Intelligence and Security Enterprise (DISE) capability to support PMs. The Defense Acquisition Intelligence focal points (organizations and/or individuals) are:

- US Office of the Under Secretary of Defense for Acquisition and Sustainment/Office the Under Secretary of Defense for Intelligence Acquisition Intelligence Division: osd.pentagon.ousd-intel.list.acq-intel.div@mail.mil
- US Air Force: usaf.pentagon.af-a2.list.af-a2o-front-office@mail.mil
- US Army: usarmy.pentagon.hqda-dcs-g-2.dami-fit-distribution@mail.mil
- US Navy: dave.a.brown1@navy.mil
- US Missile Defense Agency (MDA): joshua.littleton@mda.mil
- US Special Operations Command (USSOCOM): mark.anderson@socom.mil

CH 7–4. Threat and Intelligence Supportability

Threat is the sum of the potential strengths, capabilities and strategic objectives of any adversary that can limit or negate US mission accomplishment or reduce force, system, or equipment effectiveness. Changing threats drive the need for component resiliency and flexibility in order for systems to remain relevant in a modern battlespace. PMs will have difficulty knowing where sub-component flexibility is pertinent if they do not have good insight into where they are most vulnerable to evolving threats.

Several tools assist PMs in managing impacts from adversary threats. They include the Defense Intelligence Threat Library/threat modules, Validated On-line Life-cycle Threat (VOLT) Reports (see CH 7-5.2.1), Critical Intelligence Parameters (CIPs) (see CH7-5.2.2), Lifecycle Mission Data Plans (LMDPs) (see CH 7-5.2.3), Technology Targeting Risk Assessments (TTRAs) (see CH 7-5.2.4, Threat Systems Data Base (TSDB), and the Advanced Cyber Threat Assessment (ACTA) process.
CH 7-5 Intelligence Integration in the Acquisition Life Cycle

Today, PMs must address the changes in Defense acquisition performance required by the Acquisition Agility Act (AAA) of Fiscal Year (FY) 2017 (part of the National Defense Authorization Act of FY2017) and the focus on a more “Agile” Defense Acquisition System (DAS) that is able to respond more flexibly to dynamic threats, technology change, and capability evolution within the decision cycle of a weapons system warfighting capability program. The purpose of the changes is to modify the capabilities acquisition process to be more flexible to and to remain ahead of emerging threats; to take advantage of emerging technologies; to increase interoperability; and to reduce schedule/decrease cost. These changes include mandating a Modular Open Systems Approach (MOSA) for large warfighting capability programs, updating capability requirements descriptions, and emphasizing prototyping and experimentation outside the program of record.

PMs should look at the systems engineering and architecture of their capability to identify the sub-component areas that are most sensitive to emerging/changing threats. These components are excellent candidates for use of a MOSA where adversary threat evolution can be mitigated by sub-component evolution.

Cybersecurity is of growing importance for all acquisition efforts. The processes for ensuring adversary threats inform the cybersecurity posture of a program are rapidly evolving with best practices emerging as a result. One such best practice that can assist PMs is the ACTA. The ACTA approach has been demonstrated to provide the PM with an understanding and ability to prioritize the cyber threats and make program decisions based on factual cyber analysis.

CH 7-5.1 Materiel Solution Analysis Phase to Milestone (MS) A

Intelligence dependencies and related implications to design, performance, and test and evaluation (T&E), should be mature enough in this phase for inclusion in the Acquisition Strategy/planning and updated as design and concepts of operations change throughout the Materiel Solution Analysis Phase.

The predominantly threat intelligence requirements at MS A include the VOLT Report (including CIPs), TTRAs, and LMDP. Threat information or summaries are also integrated into other MS A requirement documents such as the Acquisition Strategy, Analysis of Alternatives (AoA), Systems Engineering Plan (SEP), Capability Development Document (CDD), Test and Evaluation Master Plan (TEMP), and Program Protection Plan (PPP).

PMs should look for insights already garnered by programs that share mission types or similar sub-components in order to leverage portfolio lessons learned about intelligence dependencies, threat impacts, and solutions to close intelligence gaps.

CH 7-5.1.1 VOLT

The VOLT Report is the authoritative threat assessment tailored for and normally focused on one specific program. A VOLT report includes threat modules and is written to articulate the relevance of each module to a specific acquisition program or planned capability.

While VOLT reports support Acquisition Category (ACAT) I-III programs, only Major Defense Acquisition Programs, Major Automated Information System programs, and programs on the Director, Operational Test and Evaluation (DOT&E) Oversight List require a unique, system-specific VOLT report to support capability development.

Exemplars of VOLT reports are available at the following Secure Internet Protocol Router Network (SIPRNet) site: https://intellipedia.intelink.sgov.gov/wiki/Validated_Online_Lifecycle_Threat_Reports

Key points:
- DoD Components produce VOLT reports and Defense Intelligence Agency (DIA) validates those produced for ACAT ID or IAM programs.

- The DoD Components approve VOLT reports for ACAT IC or IAC programs and below.

- Waiver authority for the VOLT Report is outlined in DoD Instruction (DoDI) 5000.02, Enclosure 1, paragraph 3 (VOLT Report row, Table 2).

- The process of obtaining a VOLT report includes a dialogue between all stakeholders involved with a capability development initiative.

- VOLT reports can be used to support multiple programs with similar performance attributes, share an employment concept of operations (CONOPs), and have a similar employment timeline.

- VOLT reports include program specified Critical Intelligence Parameters in order to ensure focused DISE reporting on threats that could critically impact capability.

- DIA contact information and the VOLT Report request form are available at the following SIPRNet page:

**CH 7–5.1.2 CIPs**

A CIP is a threat capability or threshold where changes to which could critically impact the effectiveness and survivability of weapon system(s). Due to their importance, CIPs receive focused intelligence analysis and reporting that can inform revisions to requirements, incremental upgrades, or potential new starts to ensure capabilities remain technologically competitive on the modern battlefield. Routine PM attention to the state of the program relative to CIPs enables risk-based decisions for program resiliency.

Exemplars of CIPs are available at the following SIPRNet site: https://intellipedia.intelink.sgov.gov/wiki/Critical_Intelligence_Parameter

**Key points:**

- CIPs submitted to Intelligence Production Centers become part of VOLT reports and monitored to keep acquisition and requirements communities informed on high priority threat developments.

- CIP development should take into account the predictive or future threat and not just the current or observed threat.

- A CIP is analogous to an objective key performance parameter for an adversarial system capability.

- CIPs are considered “breached” when adversary capability advancements overtake a parameter and effect all programs that share in the impact from that adversary advancement.

- DIA maintains a SIPRNet website to support CIP development best practices at https://intellipedia.intelink.sgov.gov/wiki/Critical_Intelligence_Parameter.

- Acquisition Intelligence Specialists annually revalidate or close CIP production requirements for the PM.

**CH7-5.1.3 LMDP**

The LMDP is the PM’s plan that articulates how the program and other organizations intend to address specific program needs for intelligence data required to operate mission systems. Typical types of data dependencies are: Characteristics and Performance (C&P) or Order of Battle data that enable prioritization and defense against enemy systems; Signatures data that enable you to detect and distinguish between friendly, neutral and enemy systems; Geospatial Intelligence (GEOINT) that provide
you mapping and locating data; Electronic Warfare Integrated Reprogramming (EWIR) data that identifies and counteracts enemy radar and detection. Gaps in data diminish the capabilities of systems and can render them vulnerable to enemy actions.

Acquisition Intelligence Specialists aid PMs in determining if they need an LMDP and assist in LMDP development. They also aid program entry into the DoD requirements prioritization and production planning processes for EWIR, Signatures, C&P, Threat Modeling and Simulation, and GEOINT products.

The Joint Staff J285 orchestrates the annual processes by which the DISE plans for production across the Future Years Defense Program of the above products and by which the Department makes risk management decisions regarding program shortfalls. In these processes, DoD Components, USSOCOM, and MDA designated requirements leads review and validate their priorities to support resource and risk management decisions.

- The Acquisition Intelligence Requirements Visualization of Enterprise Workflows (AIRViEW) tool is used to submit priority requirements for Service, MDA and USSOCOM validation and inclusion in annual intelligence production planning processes. The AIRViEW tool website is at https://intelshare.intelink.sgov.gov/sites/airview.

When there are gaps forecasted, program offices receive feedback regarding forecast shortfalls, cost, and courses of action being taken to close critical shortfalls. The Acquisition-Intelligence-Requirements Committee and GEOINT Committee meet prior to the end of the annual planning cycles to determine courses of action to support program needs and support feedback to programs regarding the status of program requirements.

**Key points:**

- The LMDP requirement begins at MS A and subsequently updated in accordance with designated life-cycle events.
- A Program Executive Officer and Component Acquisition Executive-approved draft update is due for a development request for proposal (RFP) release.
- Priorities and requirements for production planning within the Joint Staff Priorities and Risk Management Framework should contact the Joint Staff/J285 at: michael.j.simons.mil@mail.mil.
- Programs or Acquisition Intelligence specialists needing assistance in the development of LMDPs and in understanding more about intelligence mission data (IMD) production should contact DIA's Intelligence Mission Data Center at: https://intelshare.intelink.sgov.gov/sites/imdc/SitePages/Home.aspx.
- The IMD Management, Analysis, and Reporting System (IMARS) tool guides acquisition program intelligence requirements derivation for intelligence mission data needs. The IMARS tool website is at https://imars.dia.smil.mil.

**CH 7-5.1.4 TTRA**

The TTRA is a country-by-country assessment conducted by the DoD entities within the DISE that quantify risks to critical program information (CPI) and related enabling technologies for weapons systems, and advanced technologies or programs; facilities such as laboratories, factories, research and development sites (e.g., test ranges); and military installations. Its importance is as a foundation for the counterintelligence (CI) threat assessment that assesses the adversarial collection capability relative to the program’s critical information and factors in the protection of such information.

The TTRA is a MS A requirement document only for all ACAT I-III programs that have identified CPI.

**Key points:**
- The supporting Defense CI Component produces the TTRA. DIA validates the TTRA for ACAT ID and ACAT IAM programs while the DoD Component validates the TTRA for ACAT IC, IAC, and below programs.

- The process for obtaining a TTRA involves coordination between DIA and the supporting Defense CI Component which gathers programmatic information necessary to aid the analytic process.

- The TTRA forms the analytic foundation for the CI assessments (e.g., Multidiscipline CI Threat Assessment and CI Support Plan) in the PPP (see Chapter 9 of this guidebook).

- If the PM assesses the program information and does not identify CPI, the PM should document that action in a letter or memorandum to address and satisfy the TTRA MS A requirement per DoDI 5000.02, Enclosure 1, paragraph 3 (TTRA row, Table 2).

CI resource: DoDI O-5240.24, Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA), is the CI policy and procedures reference regarding support to acquisition and is available by emailing the following address: whs.pentagon.esd.mbx.dod-directives@mail.smil.mil. If CPI is not identified by MS A, the PM could satisfactorily address the TTRA requirement by issuing a memorandum stating that an assessment was conducted to identify CPI and no CPI was evident within the program at that time.

Relevant questions to consider and actions to take during this phase include:

Questions:

- In terms of the MOSA requirement, has the systems engineering and architecture of the capability been sufficiently examined to identify sub-component areas that are sensitive to emerging/ changing threat? This includes identifying opportunities for prototyping such as Rapid Fielding, Rapid Prototyping and AAA Prototyping, either as an alternative to the traditional DAS model in the case of an emergent/highly dynamic threat (e.g., Rapid Fielding) or as an adjunct to MOSA design considerations (e.g., Rapid/AAA Prototyping).

- Has consideration been given to establishing CIPs for critical components that evolved from the MOSA design process to support the threat reporting which could trigger a decision regarding critical component upgrade or modification?

- What are the evolving and forecast threat considerations? Are threat assumptions for the AoA correct? Are there any key threat considerations for attention as CIPs? Do the threshold/objective requirements make sense? Is the trade space sufficient to meet future threats? What threat representations are needed for most likely/most stressing? Are threat shortfalls captured in a foreign materiel acquisition request or is a surrogate requested?

- For each proposed material solution identified during the AoA process, will the solution require the detection and identification of an activity, event, person, material, or equipment? If yes, then for each proposed detection or identification method (radar, electro-optical/infrared (EO/IR), acoustic, chemical, etc.), assess the technical feasibility of acquiring intelligence data within cost and schedule constraints. Consider the quality of available intelligence, the capability and plans of the DISE to deliver what is needed, and whether the intelligence needs to be collected, processed and/or developed.

- Has the cyber threat been considered by using the ACTA approach? This approach has been demonstrated to provide the PM with an understanding and ability to prioritize the cyber threats and make program decisions based on factual cyber analysis. An ACTA Exemplar is available through SIPRNet channels at: https://intelshare.intelink.sgov.gov/sites/afmc-a2-master/esc_xr2/ACTA/S_NF%20AWACS%20ACTA %20 Exemplar.pptx.

- Has the program been identified for Foreign Military Sales (FMS) or Direct Commercial Sales (DCS)? If yes, then how will this affect design, development, testing, disclosure and releasability of intelligence dependent components?
CH 7-5.2 Technology Development Phase to MS B

As a program approaches MS B, the PM’s planning for supportability should become more detailed, including mission or capability-specific details that support program development. For example, as the design matures, additional details should emerge about the design of the sensors and the algorithms. The program/project might also identify any models, other production efforts (e.g. lab, warfare research center, or other agency, organization, etc.), and planned intelligence collection events from which the program will receive support.

Based on initial requirements defined for MS A, refine and add details in requirements submitted for production planning and during development of the Systems Performance Specification and the Allocated Baseline. Changes to design or risk mitigation measures resulting from planning and requirements processes should be captured in applicable documents such as the LMDP. Relative questions to consider and actions to take during this phase include:

**Questions:**

- Does the development RFP adequately translate requirements into engineering specifications?
- Any significant changes to assessments or parametric data that would impact program performance?
- For each proposed detection/identification method (radar, EO/IR, acoustic, chemical, etc.), does the required intelligence already exist (at the estimated quality needed) or will it need to be collected, processed, and produced?
- Is the required detection/identification technology sufficiently mature (Technology Readiness Level 6 or higher) to proceed into end-item design or MS B?
- Which intelligence dependent performance requirements need to be verified through operational T&E (OT&E)?
- Have Modeling and Simulation activities identified intelligence dependencies that are different from what were originally expected?
- Are intelligence dependencies reflected in digital engineering efforts and digital models?
- Do the detection/identification algorithms or processes need to be designed to accommodate Intelligence updates?
- Is there potential for the detection/identification hardware and software to perform intelligence collection and provide updates to intelligence databases? If yes, has a design study been conducted to assess feasibility and cost/benefit analysis to support the program and other weapon system needs?
- The TSDB, formerly called the Automated Joint Threat Systems Handbook, is a database and website on SIPRNET [https://tsdb.msic.dia.smil.mil](https://tsdb.msic.dia.smil.mil) maintained by the T&E Threat Resource Activity under the DOT&E. The TSDB provides information on a variety of resources for use in T&E and training. It includes threat representative systems such as simulators, targets, models and simulations, and actual threat hardware/foreign materiel. It also provides information about threat testing facilities and ranges.
- Have significant intelligence-dependent functions been included in the proposed exit criteria for the Engineering & Manufacturing Development (EMD) Phase?
- Has the program’s spectrum requirements taken into account bandwidth needed for intelligence updates during system operations and sustainment?
- Should any intelligence data sets be considered as Government Furnished Equipment for the EMD Contract?
- Has the program been identified for FMS or DCS? If yes, then how will this affect design, development, testing, disclosure and releasability of intelligence-dependent components?

CH 7-5.3 Engineering and Manufacturing Phase to MS C

If the program is transitioned to a different program office for sustainment, all intelligence data and products should also be transitioned for its continued use. The purpose is to add any new intelligence considerations resulting from design maturity or changes in the CONOPS. It should include expected
intelligence data flows for system employment in an operational environment. Documents such as the LMDP should provide information on intelligence data existing within the program (modeling and simulation or measured physical parameters) for sensor or algorithm development, or for testing purposes, and information on the existence of any US (blue) intelligence collected to support the program.

Based on intelligence support requirements defined at MS B, refine and add details for the MS C intelligence documents during development of the System Functional Specifications and the Initial Product Baseline. Relevant questions to consider and actions to take during this phase include:

Questions:

- Have threat representations been validated and accredited to support operational testing?
- Has threat changed significantly to require a re-assessment/change to the modular design?
- Is validated intelligence data available to support operational testing?
- For each proposed detection/identification method (radar, EO/IR, acoustic, chemical, etc.), has intelligence required for system operations and sustainment been planned for in the LMDP and Acquisition Strategy, at the level of quality needed?
- Which intelligence support requirements need to be verified in Follow-on OT&E?
- Has the program been identified for FMS or DCS? If yes, then how will this affect design, development, testing, disclosure and releasability of intelligence-dependent components?

CH 7-5.4 Low-Rate Initial Production to Full-Rate Production/Full Deployment Decision Review to Disposal

In preparation for initial operational capability, a requirements update is required to ensure congruence of intelligence data provision with the Final Production Baseline and to fully account for required operational needs based on the latest threat assessments and CONOPS for the system. Requirements also need to fully account for system of systems dependencies that enable operations. Combatant Command or operating unit processes for updating and fulfilling intelligence support requirements during operation and sustainment of the system are important inputs during this phase of planning for intelligence. Relevant questions to consider and actions to take during this phase include:

Questions

- Have intelligence support requirements been addressed in the Operations and Support Phase?
- Does the current CONOPS for the system drive new or updated intelligence support requirements?
- If the operational system has an intelligence reprogramming process, is the reprogramming system and organization ready for operations?
- For FMS and DCS versions of the system, have intelligence-dependent components been verified for release and authorized by the Designated Disclosure Authority?

CH 7–6. Protection/Security

While our Nation’s progress depends on the free flow of information both within the Government and to the American people, protecting information critical to our Nation’s security and demonstrating US commitment to open Government through accurate and accountable application of classification standards and routine, secure, and effective declassification are equally important priorities.

Although security is an inherent function supporting all DoD programs and activities, PMs should not underestimate the importance of identifying and protecting program information as early as possible.
CH 7–6.1 PPP

DoDI 5000.02, Enclosure 1, paragraph 3 (PPP row, Table 2) lists the PPP as a regulatory requirement at MS A through C. Details on the PPP are available in Chapter 9. It should be worth noting that CI and security play major roles in the protection or safeguarding of ACAT program information.

CH 7–6.2 Information Security

Information security is the system of policies, procedures, and requirements established in accordance with Executive Order 13526, Classified National Security Information, to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to national security. The term also applies to policies, procedures, and requirements established to protect unclassified information that may be withheld from release to the public pursuant to executive order, statute, or regulation.

Security classification guides (SCGs) are key components of classification management. Security Classification Guidance will be the PM’s main resource for implementing and administering information security practices. Refer to DoD Manual 5200.45, Instructions for Developing Security Classification Guidance, for assistance. Other best practices include the Army Classification Management Tutorial.

Questions the PM should be asking regarding information security and the protection of program information:

- Who is the Original Classification Authority (OCA) for my program information?
- Who is my information security support specialist(s)?
- Is there an SCG already developed and approved by an OCA for my program?
- If there is no approved SCG for my program, are there equivalent SCGs available within my portfolio such as aviation, ground combat systems, electronic warfare, and communications?
- Is information that is entering my program from external sources (e.g., research and development laboratories and requirement Sponsors) properly identified and marked as classified, controlled unclassified information (CUI) or public release? If not, is the PM querying the external sources on the proper identification and marking of such information? Is information used by my program inherited from another Service's program? If so, have I reviewed the SCG from which my information is inherited ensuring horizontal protection of classified information? Is the PM challenging the security classification of information deemed by the PM to be overclassified or under classified?
- If the OCA for the program information determines that there is no classified information organic to the program, has a determination been made on whether the program will have organic CUI information involved? If so, is the OCA or PM developing an SCG-equivalent guidance to inform all program stakeholders of such information?
- If the program does not involve classified information but does have CUI, how is the PM informing any contractor regarding the identification and marking of CUI? How is the PM informing the contractor regarding the safeguarding standards for CUI?
- In terms of contractor deliverables to the PM, who specifically is reviewing these items, particularly documentation, to verify that the contractor complied with the SCG and other information security guidance?

CH 7–6.3 Industrial Security

Industrial security is that portion of information security concerned with the protection of classified information in the custody of US industry.

While industrial security is a partnership between the federal government and private industry in order to protect classified information, there are also security requirements for unclassified contracts and the procedures used to ensure the safeguarding of unclassified information that are deemed sensitive or critical information. PMs must ensure that the requirements and procedures for safeguarding unclassified information are stipulated in all program contracts, as appropriate.

Questions the PM should be asking regarding industrial security and the protection of program information at cleared defense contractor facilities:

- Who is my industrial security support specialist(s)?
- Is any of my program information classified by an authorized OCA?
- How is the contractor informed of the safeguarding standards for program classified information? What is the vehicle? DD Form 254? SCG?
- Has the Defense Counterintelligence and Security Agency been informed of those most critical and/or sensitive national and commercial information assets which are entrusted to cleared industry members?
- If the program does not involve classified information but does have CUI, how is the PM informing any contractor regarding the identification, marking and safeguarding standards for CUI?
- In terms of contractor deliverables to the PM, who specifically is reviewing these items, particularly documentation, to verify that the contractor complied with the SCG and other information security guidance?

CH 7-7. References

The references cited in this table are predominantly acquisition, intelligence and security linked issuances that provide additional information to the PM and the Program Management Office staff.

<table>
<thead>
<tr>
<th>Department of Defense</th>
</tr>
</thead>
<tbody>
<tr>
<td>DoD Directive 5000.01, The Defense Acquisition System</td>
</tr>
<tr>
<td>DoD Directive 5240.01, DoD Intelligence Activities</td>
</tr>
<tr>
<td>DoD Directive 5200.43, Management of The Defense Security Enterprise</td>
</tr>
<tr>
<td>DoD Directive 5200.47E, Anti-Tamper (AT)</td>
</tr>
<tr>
<td>DoD Directive 5220.6, Defense Industrial Personnel Security Clearance Review Program</td>
</tr>
<tr>
<td>DoD Directive 5230.11, Disclosure of Classified Military Information To Foreign Governments and International Organizations</td>
</tr>
<tr>
<td>DoD Directive 5230.20, Visits and Assignments of Foreign Nationals</td>
</tr>
<tr>
<td>DoD Directive 5240.01, DoD Intelligence Activities</td>
</tr>
<tr>
<td>DoD Directive 5240.02, Counterintelligence (CI)</td>
</tr>
<tr>
<td>DoD Instruction 5000.02, Operation of the Defense Acquisition System</td>
</tr>
<tr>
<td>Document Reference</td>
</tr>
<tr>
<td>--------------------</td>
</tr>
<tr>
<td>DoD Instruction 5200.39</td>
</tr>
<tr>
<td>DoD Instruction 5200.44</td>
</tr>
<tr>
<td>DoD Instruction 5200.01</td>
</tr>
<tr>
<td>DoD Instruction 5200.02</td>
</tr>
<tr>
<td>DoD Instruction 5205.13</td>
</tr>
<tr>
<td>DoD Instruction 5220.22</td>
</tr>
<tr>
<td>DoD Instruction 5240.18</td>
</tr>
<tr>
<td>DoD Manual 5000.78</td>
</tr>
<tr>
<td>DoD Manual 5200.01, Volume 1</td>
</tr>
<tr>
<td>DoD Manual 5200.01, Volume 2</td>
</tr>
<tr>
<td>DoD Manual 5200.01, Volume 3</td>
</tr>
<tr>
<td>DoD Manual 5200.01, Volume 4</td>
</tr>
</tbody>
</table>

**Joint Chiefs of Staff**
Chairman of the Joint Chiefs of Staff Instruction 5123.01H, Charter of the Joint Requirements Oversight Council (JROC) and Implementation of the Joint Capabilities Integration and Development System (JCIDS)

Chairman of the Joint Chiefs of Staff Instruction 3901.01E, Requirements for Geospatial Information and Services, DoD Components and other Federal agencies may obtain copies of this issuance through controlled access at http://www.dtic.mil/cjcs_directives/.

Chairman of the Joint Chiefs of Staff, Manual for the Operation of the Joint Capabilities Integration and Development System (JCIDS)

**Defense Intelligence Agency**


**Department of the Air Force**


Air Force Policy Directive 16-14, Security Enterprise Governance


Air Force Instruction 63-137, Assurance of Communications Navigation, Surveillance/Air Traffic management (CNS/ATM), Navigation Safety, and Next Generation Air Transportation System (NEXTGEN) Performance

Air Force Instruction 14-111, Intelligence Support to the Acquisition Life-Cycle

Air Force Instruction 14-134, Intelligence Analysis Production and Requirements Management

Air Force Instruction 10-701, Operations Security (OPSEC)

Air Force Instruction 16-201, Air Force Foreign Disclosure and Technology Transfer Program
<table>
<thead>
<tr>
<th>Document/Manual</th>
<th>Title/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Air Force Instruction 16-1404</td>
<td>Air Force Information Security Program</td>
</tr>
<tr>
<td>Air Force Instruction 16-1406</td>
<td>Air Force Industrial Security Program</td>
</tr>
<tr>
<td>Air Force Manual 63-119</td>
<td>Certification of System Readiness for Dedicated Operational Testing</td>
</tr>
<tr>
<td>Air Force Pamphlet 63-113</td>
<td>Program Protection Planning for Life Cycle Management</td>
</tr>
<tr>
<td>Air Force Pamphlet 63-128</td>
<td>Integrated Life Cycle Management</td>
</tr>
<tr>
<td><strong>Department of the Army</strong></td>
<td></td>
</tr>
<tr>
<td>Army Regulation 70-1</td>
<td>Army Acquisition Policy</td>
</tr>
<tr>
<td>Army Regulation 70-41</td>
<td>Armaments Cooperation</td>
</tr>
<tr>
<td>Army Regulation 70-75</td>
<td>Survivability of Army Personnel and Materiel</td>
</tr>
<tr>
<td>Army Regulation 70-77</td>
<td>Program Protection</td>
</tr>
<tr>
<td>Army Regulation 380-5</td>
<td>Department of the Army Information Security Program</td>
</tr>
<tr>
<td>Army Regulation 380-10</td>
<td>Foreign Disclosure and Contacts with Foreign Representatives</td>
</tr>
<tr>
<td>Army Regulation 380-49</td>
<td>Industrial Security Program</td>
</tr>
<tr>
<td>Army Regulation 380-67</td>
<td>Personnel Security Program</td>
</tr>
<tr>
<td>Army Regulation 381-10</td>
<td>US Army Intelligence Activities</td>
</tr>
<tr>
<td>Army Regulation 381-11</td>
<td>Intelligence Support to Capability Development</td>
</tr>
<tr>
<td>Army Regulation 381-20</td>
<td>Army Counterintelligence Program (<a href="http://www.apd.army.mil">contact http://www.apd.army.mil</a>)</td>
</tr>
<tr>
<td><strong>Department of the Army Pamphlet 70-3</strong></td>
<td>Army Acquisition Procedures</td>
</tr>
<tr>
<td><strong>Department of the Navy</strong></td>
<td></td>
</tr>
<tr>
<td>Secretary of the Navy Instruction 5000.02F</td>
<td>Defense Acquisition System and Joint Capabilities Integration and Development System Implementation</td>
</tr>
</tbody>
</table>
Secretary of the Navy Instruction 5000.42, Department of the Navy Accelerated Acquisition for the Rapid Development, Demonstration and Fielding of Capability

Secretary of the Navy Instruction 5200.46, Department of the Navy Modeling, Simulation, Verification, Validation, and Accreditation Management

Secretary of the Navy Instruction 5400.15C, Department of the Navy Research and Development, Acquisition, Associated Life-Cycle Management, and Logistics Responsibilities and Accountability

Secretary of the Navy Instruction 5500.36A, Department of the Navy Security Enterprise

Secretary of the Navy Instruction 5510.30B, Department of the Navy (DON) Personnel Security Program (PSP) Instruction

Secretary of the Navy Instruction 5510.34B, Disclosure of Classified Military Information and Controlled Unclassified Information to Foreign Governments, International Organizations, and Foreign Representatives

Secretary of the Navy Instruction 5510.36A, Department of the Navy (DON) Information Security Program (ISP) Instruction

Chief of Naval Operations Instruction 3811.1F, Threat Support to the Defense Acquisition System

Chief of Naval Operations Instruction 3880.6A, Scientific and Technical Intelligence Liaison Officer (STILO) Program and Intelligence Support for the Naval Research, Development, Test & Evaluation, and Acquisition Communities

Chief of Naval Operations Instruction 5000.53A, U.S. Navy Maritime Accelerated Acquisition

CH 7–Version and Revision History

The table below tracks chapter changes. It indicates the current version number and date published, and provides a brief description of the content.

<table>
<thead>
<tr>
<th>Version #</th>
<th>Revision Date</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>2/1/17</td>
<td>Chapter 7 administrative changes</td>
</tr>
<tr>
<td>1</td>
<td>4/27/17</td>
<td>Chapter 7 administratively updated to coincide with DoDI 5000.02, CH 2, primarily establishing the VOLT and Threat Modules, and replacing the Initial Threat Environment Assessment, Capstone Threat Assessment and System Threat Assessment Report.</td>
</tr>
<tr>
<td>2</td>
<td>6/8/17</td>
<td>Chapter 7 link in paragraph 7-3.2.1.3 corrected and administrative changes made for clarification.</td>
</tr>
<tr>
<td>Revision</td>
<td>Date</td>
<td>Changes</td>
</tr>
<tr>
<td>----------</td>
<td>------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>3</td>
<td>6/26/17</td>
<td>Chapter 7 SIPRNet links in paragraphs 7-3.2.1.3 and 7-4.2.3 corrected and inserted SIPRNet links in paragraphs 7-4.1, 7-4.1.1, 7-4.1.2, and 7-4.3.2. Inserted clarifying updates to paragraphs regarding CIPs in capability documents, TTMA, intelligence manpower, CIPs in warning support, and intelligence resources. Added information on Defense Security Service role in CI support and descriptions of National Intelligence Program and Military Intelligence Program funding.</td>
</tr>
<tr>
<td>4</td>
<td>8/28/17</td>
<td>Chapter 7 SIPRNet links in paragraphs 7-3.2.1.3, 7-4.2.3 and 7-4.3.2 corrected as well as Non-secure Internet Protocol Router Network links in paragraphs 7-3.2.1.1, 7-4.1.5 and 7-S-2.</td>
</tr>
<tr>
<td>5</td>
<td>9/1/17</td>
<td>Chapter 7 additions included sections on the Threat Steering Group model, information security and industrial security.</td>
</tr>
<tr>
<td>6</td>
<td>11/22/17</td>
<td>Chapter 7 links associated with the Joint Capabilities Integration and Development System Manual corrected.</td>
</tr>
<tr>
<td>7</td>
<td>08/7/19</td>
<td>Chapter 7 update reorganized and re-formatted the chapter to focus on intelligence throughout the acquisition life cycle, to include intelligence associated with non-ACAT funded efforts. Updated and verified functioning of all links. Added a reference section at the end of the chapter with links, as appropriate.</td>
</tr>
</tbody>
</table>