Army Regulation 70–77

Research, Development, and Acquisition

Program Protection

Headquarters
Department of the Army
Washington, DC
8 June 2018

UNCLASSIFIED

SUMMARY of CHANGE

AR 70–77
Program Protection

This mandated revision, dated 8 June 2018--

- Changes the responsibilities as the primary Army headquarters responsible to conduct cyberspace operations from Second Army to United States Army Cyber Command (para. 2–7).

- Changes the definition of Critical Program Information to align it with the current definition in DODI 5200.39 (Glossary).

Headquarters
Department of the Army
Washington, DC
8 June 2018

*Army Regulation 70–77

Effective 8 June 2018

Research, Development, and Acquisition

Program Protection

By Order of the Secretary of the Army:

MARK A. MILLEY
General, United States Army
Chief of Staff

Official:

GERALD B. O'KEEFE
Administrative Assistant to the Secretary of the Army

History. This publication is a mandated revision.

Summary. This regulation provides a disciplined approach for managing the risks to advanced technology and mission- critical system functionality within Army capabilities from foreign collection, design vulnerability, supply chain exploitation, and battlefield loss.

Applicability. This regulation applies to the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated. It also applies to all acquisition activities of the Army.

Proponent and exception authority. The proponent of this regulation is the Assistant Secretary of the Army for Acquisition, Logistics and Technology. The proponent has the authority to approve exceptions or waivers to this regulation that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific guidance.

Army internal control process. This regulation contains internal control provisions in accordance with AR 11–2 and identifies key internal controls that must be evaluated (see appendix B).

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from the Assistant Secretary of the Army for Acquisition, Logistics, and Technology (SAAL–ZL), 103 Army Pentagon, Washington, DC 20310–0500.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to the Assistant Secretary of the Army for Acquisition, Logistics and Technology (SAAL–ZL), 103 Army Pentagon, Washington, DC 20310–0500.

Distribution. This regulation is available in electronic media only and is intended for the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

Contents (Listed by paragraph and page number)

*This regulation supersedes AR 70-77, dated 7 April 2014.

UNCLASSIFIED

Contents—Continued

Chapter 1
Introduction

1–1. Purpose
This regulation assigns responsibilities and prescribes policies for developing plans to protect critical program information (CPI), conducting supply-chain risk management (SCRM), and performing damage assessment activities resulting from a compromise of unclassified program information.

1–2. References
Required and related publications and prescribed and referenced forms are listed in appendix A.

1–3. Explanation of abbreviations and terms
Abbreviations and terms used in this regulation are explained in the glossary.

1–4. Responsibilities
Responsibilities are listed in chapter 2.

Chapter 2
Responsibilities

2–1. Assistant Secretary of the Army (Acquisition, Logistics and Technology)
The ASA (ALT) exercises strategic management for all acquisition program protection and damage assessment activities and will—

a. Promulgate program protection, and damage assessment policies, processes, and procedures.

b. Serve as the lead for Army's damage assessment mission.

c. Establish Army program protection objectives, goals, policies, processes, and procedures consistent with statutory and regulatory guidance.

d. Provide guidance and oversight to the research, development, and acquisition workforce ensuring program protection regulatory compliance.

e. Periodically review and evaluate the Army's program protection posture and the effectiveness of program protection plans (PPPs).

f. Promulgate policy and guidance for mitigating risks to programs involving the compromise of unclassified information residing on or transiting unclassified networks.

g. Develop and promulgate policy, processes, and procedures for trusted systems and networks (TSN).

h. Ensure acquisition personnel receive the training requisite to incorporate TSN into their respective areas of competency.

i. Ensure program executive officers appoint a program protection lead with their primary additional duty responsibilities of ensuring assigned programs have adequate program protection plans in place and are effective.

j. Ensure acquisition program managers (PMs) are in compliance with this regulation.

k. Designate a TSN focal point with access to research, development, and acquisition activities for applicable systems.

l. Develop and promulgate policy, processes, and procedures for damage assessment, critical function analysis (CFA) and CPI identification processes to include the application of countermeasures.

m. Provide authority for management and oversight of all program protection, damage assessment activities within the acquisition domain to the Deputy Assistant Secretary of the Army for Acquisition Policy and Logistics. The management and oversight includes the following:

(1) Serving as the Army TSN focal point and the office of primary responsibility for overseeing and assisting with the implementation of this policy.

(2) Establishing procedures and techniques to assess program protection management and execution.

(3) Representing the Army in all TSN meetings with the Office of the Secretary of Defense and other Department of Defense components.

(4) Ensuring program protection strategies meet protection requirements and protection plans are executable.

(5) Developing and overseeing policies for the identification CPI, critical components, and implementing TSN processes and activities.

(6) Staffing the program protection plan with applicable Department of Defense staff elements.

(7) Serving as the Army acquisition senior representative on the Intelligence Mission Data Senior Steering Group and Intelligence Mission Data Oversight Board.

(8) Serving as the life cycle mission data plan approval authority for all acquisition category programs, unless the program executive officer has been delegated as the milestone decision authority.

(9) Serving as focal point for processing requests to use other than Department of Defense intelligence components for producing weapon system intelligence mission data.

n. Providing management oversight authority for Army's system security engineer domain and strategic management to the Office of the Chief Systems Engineer. The Office of the Chief Systems Engineer falls under the ASA (ALT) and will—

(1) Serve as the Army's security engineering subject matter expert.

(2) Ensure program protection strategies use sound systems engineering disciplines and are referenced in the systems engineering plan.

(3) Assist PMs with developing program protection supporting documents and PPPs.

(4) Participate in integrated product teams for program protection activities.

(5) Inform PMs and other program participants of program protection deficiencies.

(6) Provide advice and expertise to influence system design in support of developing effective program protection strategies.

(7) Assist PMs by making recommendations to mitigate program protection risks.

(8) Participate in milestone decisions and other program reviews.

(9) Serve as office of primary responsibility and final approval authority for anti-tamper plans.

2–2. Assistant Secretary of the Army (Financial Management and Comptroller)

The ASA (FM&C) will assist Department of the Army staff in making budget decisions to support program protection and damage assessment activities.

2–3. Deputy Chief of Staff, G–2

The DCS, G–2 will—

a. Provide technology and program protection planning support as needed to Army laboratories, engineering centers, and acquisition programs.

b. Provide intelligence support to the ASA (ALT) for determining system and system of system architecture requirements to address future threats.

c. Assist the ASA (ALT) with developing processes relating to CPI that require coordination with law enforcement, security, and intelligence agencies.

d. Assist the ASA (ALT) with establishing and institutionalizing a standardized process for the identification of CPI and critical components.

e. Provide assessment regarding foreign intelligence requirements for and targeting CPI.

f. When requested by the ASA (ALT) serve as functional proponent for CFA and CPI processes to include maintaining and publishing standards.

g. Assist the ASA (ALT) to ensure appropriate training is available regarding the identification and protection of CPI.

h. When requested, assist PMs in the development and implementation of PPP for the protection of CPI, from identification until such protection is no longer required.

i. Determine the applicable staffing agencies within the DCS, G–2 organization for PPP coordination.

j. In coordination with the ASA (ALT) establish an all-source threat assessment capability to protect CPI against supply chain vulnerabilities within the Department of Defense.

k. Collaborate with the ASA (ALT) and the Chief Information Officer/G–6 (CIO/G–6) to develop guidance to mitigate risks identified in supply chain vulnerabilities.

l. Provide resources to represent Army in the threat assessment center with the mission of conducting counterintelligence analysis of suppliers identified by program offices.

m. Collaborate with the ASA (ALT) to assess the impact or likely impact of an incident in which CPI or other sensitive information was compromised by a foreign activity.

n. Respond to official inquires to provide intelligence information in support of the damage assessment process.

o. Provide counterintelligence and intelligence analytical support to the damage assessment process, including participation in damage assessment response team damage assessment activities, and provide analytical information to support all damage assessment reporting.

p. Notify the ASA (ALT) of incidents occurring on government or contractor networks that impact acquisition programs.

q. Coordinate with the ASA (ALT) and the reporting agency to provide files and information to support a damage assessment.

r. Provide a liaison to the National Cyber Investigative - Joint Task Force office to support the damage assessment processes.

2–4. Chief Information Officer/G–6

The CIO/G–6 will—

a. Integrate TSN concepts into information assurance controls and other policies and processes, as appropriate.

b. Issue guidance (for example, information system security engineering guidance) and develop programming recommendations to ensure the integration of TSN concepts and processes into the acquisition and maintenance of information systems, enclaves, and services, including the purchase and integration of information-communication technology (ICT) commodities.

c. Provide guidance and oversight to the completion and validity for the information assurance strategies.

d. Review and approve acquisition information assurance strategies prior to Milestones A, B, and C.

2–5. Commanding General, U.S. Army Training and Doctrine Command

The CG, TRADOC will—

a. Integrate approved doctrine, procedures, legalities, techniques, and methods for program protection into applicable programs of instruction for TRADOC schools.

b. Develop Army technology protection training literature and training aids, leveraging secure electronic distribution and remote-access capabilities.

c. Develop, test, and recommend operational and organizational concepts and doctrine to achieve technology protection goals.

d. Conduct or participate as applicable, in operational tests of technology protection supporting capabilities.

e. Integrate technology program protection practices into pre-Milestone A activities and other events as required.

2–6. Commanding General, U.S. Army Materiel Command

The CG, AMC will—

a. Establish a consistent and effective protection program for CPI across managed assets down through all subordinate commands.

b. Provide technology protection support to research, development, testing, and evaluation within the managed portfolio.

c. Assist functional proponents in identifying CPI protection requirements for proposed and existing weapons systems.

d. Assign responsibility to an internal agency to develop a system to track the status of potential CPI assessments for all owned technology programs.

e. Ensure all AMC subordinate commands implement adequate protection plan strategies.

f. Develop internal standard operating procedures to periodically inspect subordinate command protection plans to ensure they are in compliance with statutory and regulatory guidance.

g. Ensure anti-tamper is addressed when developing requirement documents for each Army system.

h. Provide members to various anti-tamper verification and validation boards that will determine anti-tamper requirements for systems and conduct trade-offs as necessary, ensuring that the systems can perform assigned missions while maintaining the appropriate level of anti-tamper.

2–7. Commanding General, U.S. Army Cyber Command

The CG, ARCYBER will—

a. Serve as the primary Army headquarters responsible for conducing cyberspace operations (offense cyberspace operations, defensive cyberspace operations, and Department of Defense Information Network operations) as directed and authorized on behalf of the Commander, United States Strategic Command or the Commander, United States Cyber Command.

b. Organize, train, educate, man, equip, fund, administer, deploy, and sustain Army cyber forces to conduct cyberspace operations.

Chapter 3
Program Protection

Section I

General

3–1. Policy

a. All acquisition programs will—

(1) Evaluate for CPI and develop measures for its protection. While some programs may not have CPI, every acquisition program (including those with special access content), will perform CFA to identify ICT components that require risk management to protect warfighting capabilities, capturing the protection measures in a PPP (See Department of Defense Instruction 5000.02).

(2) Conduct the intelligence mission data dependency determination process not less than 180 days prior to each milestone to determine specific system requirements, and collaborate with associated subsystem programs to determine the overall main system configuration intelligence mission data requirements. The intelligence mission data determination process is recurring and will become more detailed as the system matures through the acquisition process. The results of the determination process will be forwarded in a memorandum for record within 30 days after process completion to the Deputy Assistant Secretary of the Army for Acquisition Policy and Logistics (SAAL–ZL), 103 Army Pentagon, Washington, DC 20310–0500.

(3) Develop life cycle mission data plans on acquisition programs that are intelligence mission data dependent or have subsystems that are intelligence mission data dependent. Acquisition programs that are not intelligence mission data dependent, but have subsystem acquisition programs that are intelligence mission data dependent will develop a life cycle mission data plan (roll-up), reflecting the overall system intelligence mission data shortfalls and associated risk to capability at the major end item system level. The life cycle mission data plan will be developed, assembled, updated, managed, and shared on the secure internet protocol router network (See Department of Defense directive 5250.01).

b. The PPP and any associated documents will be marked and controlled in accordance with the program's security classification guide. The PPP will be developed, assembled, updated, managed, and shared on the secure internet protocol router network. The PPP should be classified by content. Threat and vulnerability information is commonly classified at "SECRET" or above. Detailed descriptions of CPI and critical functions and components may also be classified.

c. PPP staffing and request for approval will commence not less than 180 days prior to the next milestone or as directed by the milestone decision authority. *Note*. Due to the shorter acquisition cycle times of agile and cyber acquisition programs, submission of their PPP may need to be adjusted. However, managers of agile and cyber acquisition programs need to coordinate directly with other document proponents to define shortened approval processes.

d. PPPs will be uploaded into the acquisition security database to enable comparative analysis of defense systems' technologies and align Army CPI protection activities horizontally throughout the Department of Defense.

e. New contracts supporting acquisition programs where CPI or ICT critical components have been identified, will contain contractual terms requiring the contractor to implement protection measures. This includes incorporating language in request for proposals that require their defense industrial base partners and all tiers of contractors supporting the weapon system to develop and implement measures for protecting program information on their networks.

3–2. Program protection plan applicability

a. All acquisition category programs containing CPI or ICT critical components are required to submit a PPP for milestone decision authority or equivalent approval. This requirement also applies to systems acquired or procured through quick reaction capability or rapid equipping force initiatives. For these type acquisitions and procurements, the milestone decision authority is the PPP approval authority. The PPP document, to include annexes will be uploaded into the acquisition security database.

b. Programs that do not have CPI or ICT critical components will submit a memorandum for record, endorsed by the milestone decision authority into the acquisition security database documenting the results of the CPI assessment and CFA.

c. PPPs or updated PPPs (if the program has an existing PPP) are required at each milestone and full rate production or full deployment decisions or as directed by the milestone decision authority.

d. The PPP will be updated annually after the full rate production or full deployment decision.

e. Programs involved in a damage assessment due to an actual or potential compromise incident will review their PPP and update it as applicable to address vulnerabilities and mitigate risks. Programs without a PPP that are involved in a damage assessment will develop a PPP to address vulnerabilities and mitigate risks.

f. Requests for exceptions to paragraphs 3–1 and 3–2 are as follows:

(1) PMs who determine that the PPP requirement does not apply to their program must request a waiver from the Deputy Assistant Secretary of the Army for Acquisition Policy and Logistics (SAAL–ZL), 103 Army Pentagon, Washington, DC 20310–0500.

(2) If the request is granted, the requesting PM may not extend such authorization to additional programs. The exception will expire one year from the date of approval.

3–3. Program protection plan outline

a. The program protection outline will guide PMs through a systematic process to assist in developing their PPP. PMs must have a full understanding of what requires protecting and develop a plan accordingly. Once a PPP is in place, it should guide the program office security measures and be updated and approved by the milestone decision authority prior to the milestone, or as threats and vulnerabilities change or are better understood.

b. The following outline will be used for developing a PPP:

(1) Introduction - Purpose and update plan.
(a) Technology or system description.
(b) Program protection responsibilities.
(2) Program protection summary.
(a) Schedule.
(b) CPI and critical functions and components protection.
(3) CPI and critical components.
(a) Identification methodology.
(b) Inherited CPI and critical components.
(c) Organic CPI and critical components.
(4) Horizontal protection.
(5) Threats, vulnerabilities, and countermeasures.
(a) Threats.
(b) Vulnerabilities.
(c) Countermeasures.
(6) Other system security related plans and documents.
(7) Program protection risks.
(8) Foreign involvement and defense exportability features.
(9) Processes for management and implementation of PPPs.
(a) Audits and/or inspections.
(b) Engineering and/or technical reviews.
(c) Verification and validation.
(d) Sustainment.
(10) Processes for monitoring and reporting compromises.
(11) Program protection costs.
(a) Security costs.
(b) Acquisition and systems engineering protection costs.

c. The PPP will also include the following documents as appendixes:

(1) Appendix A: Security classification guide.
(2) Appendix B: Counterintelligence support plan.
(3) Appendix C: Criticality analysis.
(4) Appendix D: Anti-tamper plan.
(5) Appendix E: Acquisition information assurance strategy.

d. The PPP input may be tailored to accommodate sections not applicable to a system or program, however the PM must justify the exclusion of any topics or appendix within the PPP.

Section II

Trusted Systems and Networks

3–4. General

a. Overview. TSN are created in part through SCRM, a systematic process that identifies susceptibilities, vulnerabilities, and threats associated with mission-critical ICT (that is, integrated circuits, software, and firmware) throughout the

supply chain and the development of mitigation strategies to combat those threats whether presented by the supplier, the supplied product and its subcomponents, or the supply chain infrastructure.

b. Goal. The TSN goal is to achieve reliable and uncompromised mission critical systems by applying a combination of disciplines such as supply chain risk management, software assurance, information cybersecurity, information assurance, systems security engineering, and operations security when acquiring ICT.

3–5. Supply chain risk management

SCRM is a systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities, and threats throughout the supply chain and developing mitigation strategies to combat those threats whether presented by the supplier, the supplied product and its subcomponents, or the supply chain. SCRM will be applied to all information systems and weapons systems that are designated as, or comprised of, any of the following:

a. National Security Systems, Automated Tactical Systems, and automated weapon systems as defined by Army regulation 25–2.

b. Mission Assurance Category I systems, as defined by Department of Defense Instruction 5200.44.

c. Systems registered as mission critical in Army portfolio management system or the Department of Defense's information technology repository.

d. Other systems that the Army Acquisition Executive or CIO/G–6 determines are critical to the direct fulfillment of military or intelligence missions.

3–6. Supply-chain risk management process

The SCRM process is conducted through the following steps:

a. Perform CFA and identify ICT components with associated suppliers.

b. Request threat analysis of suppliers of critical components. *Note.* All threat analysis of suppliers will be managed on the secret internet protocol router network.

c. Review supplier threat information and conduct a vulnerability assessment, focusing on areas such as verified trusted producer, extent of trusted supplier or original equipment manufacturer involvement, distribution, and supply channels outside the trusted environment, and production outside the trusted wholesale supply process.

d. Determine initial risk based on the vulnerability assessment and supplier threat.

e. Identify and apply countermeasures.

f. Measure and document activities to include the residual risk in the PPP.

Section III

Critical Functional Analysis

3–7. Overview

a. CFA is the key SCRM scoping process that identifies system mission critical functions and then maps those functions to the associated ICT components and subcomponents, to include components and subcomponents that defend or have unmediated access to mission critical components.

b. CFA is an iterative, functional, and technical decomposition of the system which involves:

(1) Identifying and prioritizing system mission threads.

(2) Decomposing the mission threads into their mission critical functions.

(3) Identifying the system components (hardware, software, and firmware) that implement those functions (that is, components that are critical to the mission effectiveness of the system or an interfaced network).

c. PMs will conduct an initial program CFA during pre-Milestone A activities and throughout the system's life cycle. Each CFA iteration will build on the previous iteration, so that the protection strategy becomes more comprehensive as the system design and supportability features mature. Knowledge gained from prior analyses will be used to update the risk assessment information, and threat and vulnerability assessments. At a minimum, the PM will conduct the CFA process—

(1) Prior to Milestone A to evaluate mission threads, identify system functions, and analyze notional system architectures to identify mission critical functions.

(2) Prior to Milestone B to refine the critical function list and identify critical system components and candidate subcomponents consisting of hardware, software, and firmware.

(3) Prior to the critical design review to analyze the detailed design or architecture and update the list to identify all critical system components and subcomponents.

d. The PM will work with contracting officers to ensure language in request for proposals requires contractors to perform updated CFAs periodically, based on previous CFAs. The CFA will be led by systems engineers or persons with equivalent system expertise.

3–8. Critical function analysis procedural steps

a. The CFA process is subjective and may require adjustments be made to those items identified as critical functions and subsequently their ICT critical components. The system capability developer should be consulted to verify the critical functions from a warfighter's perspective.

b. Results of the CFA will support completing the threat assessment requests. The CFA procedural steps are as follows:

(1) The program team, led by the system engineer (or person determined to have the required expertise) will determine the high-level mission categories or capabilities (for example, command, control, and communications, situational awareness, lethality, or survivability) that apply to the system. Mission categories are used to determine prioritization of critical components.

(2) Identify the critical functions that apply to each applicable mission or capability category.

(3) Identify the hardware and software ICT components performing or enabling each critical function.

(4) For all hardware and software ICT components—

(a) Assess system impact in the event a compromise occurs.

(b) Determine the type of products and whether legacy or program specific (for example, commercial off-the-shelf, Government off-the-shelf, or developmental item).

(c) Determine the failure criticality level for each critical component. Once the functions are identified and the components and subcomponents mapped, the PM will assign levels of criticality commensurate with the consequence of their failure on the system's ability to perform its mission (see the Defense Acquisition Guidebook).

c. The PM will ensure the output of CFA effectively identifies critical elements for inclusion in a threat analysis request to include the following:

(1) A complete list of mission-critical functions and components.

(2) Criticality level assignments for all items in the list.

(3) Rationale for inclusion or exclusion from the list.

(4) Supplier information for each critical component.

d. The identification of critical functions, critical components, and the assessment of system impact if compromised must be summarized in appendix C of the PPP.

e. ICT critical components from the CFA process will be used as inputs to the threat assessment, vulnerability assessment, risk assessment, and countermeasure selection.

Section IV

Other Associated Protection Policies

3–9. Foreign involvement

a. Defense exportability features is an effort established to develop and incorporate technology protection features into a system or subsystem during its research and development phase. PMs will evaluate pursuing exportable versions of a system or subsystem that could be sold earlier in the production and development phase. This strategy may enable the capability to be available to allies and friendly companies more rapidly and lower the unit cost of procurements.

b. Prior to the engineering and manufacturing development phase, PMs will investigate the necessity and feasibility (from cost, engineering, and exportability perspectives) of the design and development of differential capability and enhanced protection of exportable versions of the system or subsystem.

3–10. Special access programs

If the special access program or system contains CPI, the PM will prepare and implement a PPP prior to transitioning to collateral or unclassified status. Security, intelligence, and counterintelligence organizations should assist in developing the PPP. The PPP will be provided to the offices responsible for implementing protection requirements before beginning the transition.

3–11. Anti-tamper

a. General. Anti-tamper is a system engineering activity that will be initiated at the earliest possible opportunity in a program's requirements definition phase. Anti-tamper involves risk analysis, and the PM's decision not to implement anti-

tamper must be based on risks involved as well as on other factors including, but not limited to, feasibility, cost, performance impacts on the system, and schedule impacts. The goal of anti-tamper is to deter the reverse engineering and exploitation of critical technology or CPI by impeding technology transfer, stopping alteration of system capability, thus preventing the development of countermeasures to weapon systems resulting from unintentional transfer of critical technology or CPI. This will be achieved through a rigorous process to identify and quantify probable system critical technology or CPI in their expected operating environments and deploy measurers that mitigate risks.

b. Scope and applicability. This anti-tamper policy applies to system performance, materials, hardware, software, algorithms, design, and production methods, maintenance, and logistical support, and other facets as determined by competent acquisition authority. If anti-tamper is determined applicable to the system, the PM will establish a plan to maintain anti-tamper protection throughout the system using documentation, training, configuration controls and verification. The anti-tamper protection of each system will be maintained throughout its life cycle as an integral activity of normal maintenance.

c. Cost. The costs associated with engineering anti-tamper protective measures into weapon systems will be borne by all users of the system, including foreign users, subject to any applicable Department of Defense financial management regulatory restrictions.

Chapter 4
Damage Assessment

4–1. Purpose
Damage assessment is a process designed to determine the cost, schedule, performance, or operational impacts to acquisition programs and activities resulting from an incident of unauthorized access to system information on unclassified networks or potential compromise or modification of data on current and future weapons programs, scientific and research projects, and warfighting capabilities.

4–2. Documenting results
The results of the damage assessment will be captured by the applicable PM in an updated PPP or an incident memorandum if the program does not meet the criteria for a PPP in accordance with this regulation. The damage assessment results will include the following:

a. Description of the Army information compromised.
b. Program impacts due to the compromise.
c. A synopsis of mitigation and/or remediation activities taken.
d. Plan for mitigation if not complete.
e. Recommendations for further action or analysis, as appropriate.

4–3. Requirements for open incidents
PMs with open incidents will provide an update to the Deputy Assistant Secretary of the Army (Acquisition Policy and Logistics) annually on the status of completing their program's mitigation and remediation activities until the incident assessment is closed.

4–4. Closing incidents
Damage assessment incidents are considered closed when the all remediation activities are accomplished. PMs that have completed remediation activities, will forward the program PPP or incident closure memorandum request (if the program does not meet the requirements for a PPP) to the Deputy Assistant Secretary of the Army (Acquisition Policy and Logistics) (SAAL–ZL), 103 Army Pentagon, Washington, DC 20310–0103.

Appendix A

References

Section I

Required Publications

AR 25–2
Information Assurance (Cited in para 3–5*a*.)

DODI 5200.44
Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN) (Cited in para 3–5*b*.) (Available at http://www.dtic.mil/whs/directives/.)

Section II

Related Publications

A related publication is a source of additional information. The user does not have to read it to understand this publication. DOD publications are available at http://www.dtic.mil/whs/directives/.

AR 11–2
Managers' Internal Control Program

AR 25–30
The Army Publishing Program

Defense Acquisition Guidebook
Program Protection (Available at https://acc.dau.mil/communitybrowser.aspx?id=492074.)

DODD 5250.01
Management of Intelligence Mission Data (IMD) in DoD Acquisition

DODI 5200.39
Critical Program Information (CPI) Protection within Research, Development, Test and Evaluation (RDT&E)

DODI 5000.02
Operation of the Defense Acquisition System

Section III

Prescribed Forms

This section contains no entries.

Section IV

Referenced Forms

Unless otherwise indicated, DA Forms are available on the APD Web site (http://www.apd.army.mil).

DA Form 11–2
Internal Control Evaluation Certification

DA Form 2028
Recommended Changes to Publications and Blank Forms

Appendix B

Internal Control Evaluation

B–1. Function
The function covered by this evaluation is program protection.

B–2. Purpose
The purpose of this evaluation is to assist system managers in evaluating program protection planning and implementation.

B–3. Instructions
Answers must be based upon the actual testing of controls (for example, document analysis, direct observation, sampling, simulation, and/or others). Answers that indicate deficiencies must be explained and the corrective action indicated in the supporting documentation. These internal controls must be evaluated annually and then certified on DA Form 11–2 (Internal Control Evaluation Certification).

B–4. Test questions
a. Have all critical functions and components been identified?
b. Has new technology been evaluated for the existence of CPI?
c. Has the PPP been reviewed in the past year to address any changes to the system or threat environment?
d. If required, has an anti-tamper plan been developed and implemented?
e. Is the system preparing to undergo a modification or upgrade that will drive a review of the PPP and was it accomplished?
f. Was SCRM incorporated into program protection and information technology procurement activities?
g. Was the CFA process used to identify critical components and vendors?
h. Were threats, vulnerabilities, and countermeasures updated during the most recent PPP review?
i. Has the system or technology been evaluated for international involvement?
j. Have all the system threats been identified?
k. Has a vulnerability assessment been completed?
l. Has information assurance been adequately addressed?
m. Has software assurance been adequately addressed?
n. Have countermeasures been implemented and are they effective?
o. Have risk mitigations been applied and are they effective?
p. Have protection requirements been included in contract updates?

B–5. Supersession
Not applicable.

B–6. Comments
Help make this a better tool. Submit comments to the Assistant Secretary of the Army (Acquisition, Logistics and Technology) (SAAL–ZL), 103 Army Pentagon, Washington, DC 20310–0103.

Glossary

Section I

Abbreviations

AMC
U.S. Army Material Command

ARCYBER
U.S. Army Cyber Command

ASA (ALT)
Assistant Secretary of the Army (Acquisition, Logistics and Technology)

ASA (FM&C)
Assistant Secretary of the Army (Financial Management and Comptroller)

CFA
critical function analysis

CG
commanding general

CIO/G–6
Chief Information Officer/G–6

CPI
critical program information

DCS, G–2
Deputy Chief of Staff, G–2

ICT
information-communication technology

PM
program manager

PPP
program protection plan

SCRM
supply chain risk management

TRADOC
U. S. Army Training and Doctrine Command

TSN
trusted systems and networks

Section II

Terms

Anti–tamper
Anti-tamper is defined as the systems engineering activities intended to prevent and/or delay exploitation of critical technologies in U.S. weapon systems.

Automated tactical system
Any information system that is used for communications, operations, or as a weapon during mobilization, deployment, or a tactical exercise. An automated tactical system may include, but is not limited to, data processors, firmware, hardware, peripherals, software, or other interconnected components and devices (for example, radar equipment, global positioning devices, sensors, and guidance systems for airborne platforms).

Automated weapon systems
Any weapon system that utilizes a combination of computer hardware and software to perform the functions of an information system (such as collecting, processing, transmitting, and displaying information) in its operation.

Critical function analysis
A key supply chain risk management scoping process that identifies system mission-critical functions and then maps those functions to the associated information communication and technology components and subcomponents, to include components and subcomponents that defend or have unmediated access to mission-critical components.

Critical program information
U.S. capability elements that contribute to the warfighters' technical advantage, which if compromised, undermines U.S. military preeminence. U.S. capability elements may include, but are not limited to, software algorithms and specific hardware residing on the system, its training equipment, or maintenance support equipment. (see Department of Defense Instruction 5200.39).

Functional proponent
The proponent or office with responsibility for certifying that a process or activity has been performed accurately and meets established standards.

Hardware
The physical, touchable, material parts of a computer or other system. The term is used to distinguish these fixed parts of a system from the more changeable software or data components it executes, stores, or carries. Computer hardware typically consists chiefly of electronic devices (central processing unit, memory, and display) with some electromechanical parts (keyboard, printer, disk drives, tape drives, and loudspeakers) for input, output, and storage.

Information–communication technology
Includes all categories of ubiquitous technology used for the gathering, storing, transmitting, retrieving, or processing of information (for example, microelectronics, printed circuit boards, computing systems, software, signal processors, mobile telephony, satellite communications, and networks). Information-communication technology is not limited to information technology; rather this term reflects the convergence of information technology and communication.

Special access program
A sensitive program, approved in writing by a head of agency with original top secret classification authority, that imposes need-to-know and access controls beyond those normally provided for access to CONFIDENTIAL, SECRET, or TOP SECRET information. The level of controls is based on the criticality of the program and the assessed hostile intelligence threat. The program may be an acquisition program, an intelligence program, or an operations and support program.

Supply chain risk management
The management of supply chain risk whether presented by the supplier, the supplied product and its subcomponents or the supply chain (for example, packaging, handling, storage, and transport).

Trusted systems and networks
The integration of systems engineering, supply chain risk management, security, counterintelligence, intelligence, information assurance, hardware, and software assurance, and information systems security engineering disciplines into a single overarching strategy.

Section III

Special Abbreviations and Terms
This section contains no entries.