

Army Regulation 525–2

Military Operations

The Army Protection Program

**Headquarters
Department of the Army
Washington, DC
9 June 2023**

UNCLASSIFIED

SUMMARY of CHANGE

AR 525–2

The Army Protection Program

This administrative revision, dated 24 July 2023—

- o Clarifies responsibilities for the Chief Information Officer and Deputy Chief of Staff, G–6 (paras 2–8 and 2–15).

This major revision, dated 9 June 2023—

- o Adds responsibilities for the Vice Chief of Staff of the Army (para 2–1).
- o Identifies the Chief Information Officer as the proponent responsible for cybersecurity (para 2–8).
- o Updates the responsibilities for the Chief Information Officer (para 2–8).
- o Updates responsibilities assigned to the Deputy Chief of Staff, G–2 (para 2–12).
- o Assigns the Deputy Chief of Staff, G–3/5/7 responsibility to manage the Army Protection Program (para 2–13*b*).
- o Includes the Army User Activity Monitoring Program, a function of the Army Insider Threat Program, under the auspices of the Deputy Chief of Staff, G–6 and the Commanding General, U.S. Army Cyber Command (paras 2–15 and 2–27).
- o Updates responsibilities for the Deputy Chief of Staff, G–6 (para 2–15).
- o Updates responsibilities for the Deputy Chief of Staff, G–9 (para 2–17).
- o Directs the Provost Marshal General to specify O–5 level representation in the Army Protection Program Working Group and updates responsibilities (para 2–24).
- o Requires the Director, U.S. Army Criminal Investigation Division, to provide law enforcement and criminal intelligence information to the Army Insider Threat Hub (para 2–28).
- o Establishes the Army Protection Program Working Group (para 3–3).
- o Clarifies the purpose and operation of the Army Protection Program Working Group, as part of the Army Protection Program Governance Cycle (app C).
- o Updates exercise requirement to triennial exercise of all Army Primary Protection primary functions (para D–1*g*).
- o Updates terms and definitions (glossary).
- o Changes (G–34) to DAMO–ODP (G–34) to reflect the current status of Protection as a Division (G–34) within the Operations, Readiness, and Mobilization Directorate (throughout).


Effective 9 July 2023

Military Operations
The Army Protection Program

By Order of the Secretary of the Army:

JAMES C. MCCONVILLE
General, United States Army
Chief of Staff

Official:


MARK F. AVERILL
Administrative Assistant to the
Secretary of the Army

History. This publication is an administrative revision. The portions affected by this administrative revision are listed in the summary of change.

Summary. This regulation prescribes policy, procedures, and assigns responsibilities for the Army Protection Program to better manage risks relative to the security of our personnel, infrastructure, and information. It prescribes policies, roles, and responsibilities, and relationships across the Army Protection Program primary and enabling functions.

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.

Proponent and exception authority. The proponent for this regulation is the

Deputy Chief of Staff, G-3/5/7. 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 requirements.

Army internal control process. This regulation contains internal control provisions and identifies key internal controls that must be evaluated (see appendix E).

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from the Deputy Chief of Staff, G-3/5/7, 400 Army Pentagon, Washington, DC 20310-0400.

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 Deputy Chief of Staff G-3/5/7 (DAMO-OD), 400 Army Pentagon, Washington, DC 20310-0400 or USARMY Pentagon HQDA DCS G-3/5/7 Mailbox AOC G34 SPP Branch at usarmy.pentagon.hqda-dcs-g-3-5-7.list.aoc-g34-all@army.mil.

Committee management. AR 15-39 requires the proponent to justify establishing/continuing committee(s), coordinate draft publications, and coordinate changes in committee status with the Office of the Administrative Assistant to the Secretary of the Army, Special Programs Directorate at email usarmy.pentagon.hqda-hsa.mbx.committee-management@army.mil. Further, if it is determined that an established "group" identified within this regulation later takes on the characteristics of a committee as found in AR 15-39, then the proponent will follow AR 15-39 requirements for establishing and continuing the group as a committee.

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)

Chapter 1

Introduction, page 1

Purpose • 1-1, *page 1*

References and forms • 1-2, *page 1*

Explanation of abbreviations and terms • 1-3, *page 1*

Responsibilities • 1-4, *page 1*

Records management (recordkeeping) requirements • 1-5, *page 1*

Statutory authority • 1-6, *page 1*

Civil liberties • 1-7, *page 1*

Precedence • 1-8, *page 1*

*This publication supersedes AR 525-2, dated 8 December 2014.

Contents—Continued

Chapter 2

Responsibilities, *page 1*

Vice Chief of Staff of the Army • 2–1, *page 1*

Assistant Secretary of the Army (Acquisition, Logistics and Technology) • 2–2, *page 2*

Assistant Secretary of the Army (Financial Management and Comptroller) • 2–3, *page 2*

Assistant Secretary of the Army (Installations, Energy and Environment) • 2–4, *page 2*

Assistant Secretary of the Army (Manpower and Reserve Affairs) • 2–5, *page 2*

The General Counsel • 2–6, *page 2*

The Administrative Assistant to the Secretary of the Army • 2–7, *page 2*

The Chief Information Officer • 2–8, *page 3*

The Inspector General • 2–9, *page 3*

Director of the Army Staff • 2–10, *page 3*

Deputy Chief of Staff, G – 1 • 2–11, *page 3*

Deputy Chief of Staff, G – 2 • 2–12, *page 3*

Deputy Chief of Staff, G – 3/5/7 • 2–13, *page 4*

Deputy Chief of Staff, G – 4 • 2–14, *page 5*

Deputy Chief of Staff, G–6 • 2–15, *page 5*

Deputy Chief of Staff, G – 8 • 2–16, *page 5*

Deputy Chief of Staff, G – 9 • 2–17, *page 5*

Chief, National Guard Bureau • 2–18, *page 5*

Chief of Army Reserve • 2–19, *page 5*

Chief of Engineers • 2–20, *page 6*

The Surgeon General • 2–21, *page 6*

The Judge Advocate General • 2–22, *page 6*

Chief of Chaplains • 2–23, *page 6*

The Provost Marshal General • 2–24, *page 6*

Commanders of Army commands, Army service component commands, and direct reporting units • 2–25, *page 6*

Commanding General, U.S. Army Training and Doctrine Command • 2–26, *page 6*

Commanding General, U.S. Army Cyber Command • 2–27, *page 6*

Director, U.S. Army Criminal Investigation Division • 2–28, *page 7*

Commanding General, U.S. Army Corps of Engineers • 2–29, *page 7*

Chapter 3

The Army Protection Program, *page 7*

Army Protection Program functions • 3–1, *page 7*

The Army Protection Program implementation • 3–2, *page 8*

Army Protection Program Governance Cycle, at Headquarters Department of the Army • 3–3, *page 9*

Chapter 4

Headquarters, Department of the Army, *page 10*

Army Protection Program activities at Headquarters, Department of the Army • 4–1, *page 10*

Planning, Programming, Budgeting, and Execution cycle • 4–2, *page 10*

Army Protection Program assessments • 4–3, *page 11*

Chapter 5

Commands, Agencies, Activities, and Installations, *page 11*

Planning and integration • 5–1, *page 11*

Training • 5–2, *page 13*

Exercise integration • 5–3, *page 13*

Assessing • 5–4, *page 13*

Evaluating • 5–5, *page 14*

Appendixes

A. References, *page 15*

B. The Army Protection Program Functions, *page 21*

Contents—Continued

- C. Army Protection Program Governance Cycle at Headquarters, Department of the Army, *page 25*
- D. Integrated Protection Plan Format for Commands, Agencies, Activities and Installations, *page 28*
- E. Internal Control Evaluation, *page 30*

Figure List

Figure 3–1: Army Protection Program’s Functions, *page 8*

Glossary

Chapter 1

Introduction

1–1. Purpose

This regulation establishes the Army Protection Program (APP) to better manage risks to the Army, including the safety and security of Soldiers, DA Civilians, Family members, contractors, facilities, infrastructure, and information. The APP provides the overarching governance framework for synchronizing, integrating, coordinating, and prioritizing policies, decisions, and resources of the 13 APP primary functions, 3 subordinate functions, and 3 enabling functions identified in paragraph 3–1. This regulation prescribes policies, roles, responsibilities, and relationships across the APP Functions. The APP applies risk management processes to integrate and coordinate protection programs into Army operations, expand program oversight, ensure senior leader accountability, and better facilitate informed decision-making and resource allocation.

1–2. References and forms

See appendix A.

1–3. Explanation of abbreviations and terms

See glossary.

1–4. Responsibilities

Responsibilities are listed in chapter 2.

1–5. Records management (recordkeeping) requirements

The records management requirement for all record numbers, associated forms, and reports required by this regulation are addressed in the Record Retention Schedule–Army (RRS–A) and/or the Army Records Disposition Schedule. Detailed information for all related record numbers, forms, and reports are located in Army Records Information Management System (ARIMS)/RRS–A at <https://www.arims.army.mil>. If any record numbers, forms, and reports are not current, addressed and/or published correctly in ARIMS/RRS–A, see DA Pam 25–403 for guidance.

1–6. Statutory authority

Title 10, United States Code, Section 7013 (10 USC 7013) provides the statutory authority for this regulation.

1–7. Civil liberties

The APP respects privacy and civil liberties while accomplishing the Army’s mission. This regulation addresses activities where the Army obtains, shares, and uses information in the interest of protecting persons, property, and other functions of national security. By following U.S. laws and Department of Defense (DoD) and Army policies through the APP, the Army’s leadership provides oversight to ensure no encroachment on civil liberties while collecting information. The APP will apply AR 25–22 and AR 25–55 to all aspects of the protection planning and assessment.

1–8. Precedence

This regulation is the proponent policy document for the APP. All other policies, including but not limited to regulations, and/or Army directives of the APP functions will comply with this regulation. If at any time there is a conflict in this regulation with any other APP-related Army policy, this regulation takes precedence.

Chapter 2

Responsibilities

The responsibilities listed in this regulation specifically support the APP and supplement other responsibilities in applicable directives, policies, regulations, or laws. All persons designated as Headquarters, Department of the Army (HQDA) Army Protection Program Board of Directors (APPBOD) board members by the Secretary of the Army, and all commanders, Army organizations, and personnel will support the Deputy Chief of Staff (DCS), G–3/5/7 in executing this regulation and implementing the APP.

2–1. Vice Chief of Staff of the Army

The VSCA will—

a. Advise and assist the Chief of Staff of the Army to develop and implement policies and procedures for the Army Special Access Programs (SAP) Central Office related to the APP personnel security, information security, industrial security, to enable the APP.

b. In coordination with the DCS, G-2, the DCS, G-6, and the Chief Information Officer (CIO), oversee Army SAP synchronization with the Army Insider Threat Program and affiliated operations.

2-2. Assistant Secretary of the Army (Acquisition, Logistics and Technology)

The ASA (ALT) will—

a. Serve as a member of the APPBOD and provide representation to the Army Protection Program General Officer Steering Committee (APPGOSC), the Army Protection Program Council of Colonels (APPCOC), and the Army Protection Working Group (APPWG), as appropriate.

b. Provide subject matter experts (SMEs) to assist the DCS, G-3/5/7 in synchronizing protection-related acquisition issues. Incorporate necessary protection measures into the contract support process and directives.

c. Assign a Department of the Army (DA) system coordinator for all centrally managed APP acquisition programs to ensure interoperability between programs with new materiel fielding and integration with related DoD, Joint Staff (JS), and other Army acquisition protection programs.

2-3. Assistant Secretary of the Army (Financial Management and Comptroller)

The ASA (FM&C) will—

a. Serve as a member of the APPBOD and provide representation to the APPGOSC, APPCOC, and APPWG, as appropriate.

b. Assist the DCS, G-3/5/7, DAMO-ODP (G-34) in coordinating fiscal management recommendations for the APPBOD.

c. Ensure that the Army budget process considers Army protection priorities when making decisions regarding protection-related management decision packages (MDEPs).

d. Provide SMEs to assist the DCS, G-3/5/7, DAMO – ODP (G-34) in synchronizing protection-related issues influencing multiple MDEPs and program evaluation groups (PEGs) to reduce redundant efforts across the APP.

2-4. Assistant Secretary of the Army (Installations, Energy and Environment)

The ASA (IE&E) will—

a. Serve as a member of the APPBOD and provide representation to the APPGOSC, APPCOC and APPWG, as appropriate.

b. Assist the DCS, G-3/5/7, DAMO – ODP (G-34) in coordinating prioritization of APP policies, directives, and programs associated with installations, critical infrastructure, sustainability, and energy security for the APPBOD.

c. Provide SMEs to assist the DCS, G-3/5/7 in synchronizing protection-related issues influencing multiple MDEPs and PEGs to reduce redundant programs across the APP.

2-5. Assistant Secretary of the Army (Manpower and Reserve Affairs)

The ASA (M&RA) will—

a. Develop policy for and exercise oversight of the APP and ensure the close coordination of oversight efforts across the Secretariat, particularly with the ASA (FM&C) and the ASA (IE&E) to properly address fiscal and installation concerns.

b. Serve as a co-chair of the APPBOD and provide representation to the APPGOSC, APPCOC, and APPWG, as appropriate.

c. Advise and assist the DCS, G-3/5/7 in fulfilling protection-related responsibilities.

d. Provide oversight of training, readiness, manpower, and other APP-related issues.

2-6. The General Counsel

The GC will serve as a member of the APPBOD and provide representation to the APPGOSC, the APPCOC and the APPWG, as appropriate.

2-7. The Administrative Assistant to the Secretary of the Army

The AASA will—

a. Serve as a member of the APPBOD and provide representation to the APPGOSC, the APPCOC, and the APPWG, as appropriate.

- b.* Implement the APP for HQDA/OA–22 assigned organizations in the National Capital Region by performing the responsibilities listed in chapter 5 of this regulation applicable to a headquarters.
- c.* Conduct triennial assessments of HQDA/OA–22 assigned organizations in the National Capital Region to assess proper implementation and compliance with the APP.

2–8. The Chief Information Officer

The CIO will—

- a.* Serve as a member of the APPBOD and provide representation to the APPGOSC, APPCOC, and APPWG, as appropriate.
- b.* Issue policies and guidance for Army cybersecurity activities to support DODIN operations in support of APP as described in DODI 8530.01.
- c.* Set the strategic direction and policy, and verify that enterprise resources are used effectively for Armywide activities, to design, build, configure, secure, operate, maintain, modernize, and sustain the Army-managed portion of the DODIN.

2–9. The Inspector General

The IG may provide inspection reports upon request that include findings related to the APP primary protection functions or enabling functions. All reports provided by the IG will be controlled classified information or will be classified, as appropriate. The IG will redact those reports as necessary. Reports will not be disseminated to agencies outside the Army without the consent of the IG.

2–10. Director of the Army Staff

The DAS will serve as a member of the APPBOD and provide representation to the APPGOSC, APPCOC, and APPWG, as appropriate.

2–11. Deputy Chief of Staff, G–1

The DCS, G–1 will—

- a.* Serve as a member of the APPBOD and provide representation to the APPGOSC, APPCOC and APPWG.
- b.* Serve as the APP lead for the Army Suitability Program in accordance with AR 600–78.
- c.* Facilitate the sharing of human resources information with cybersecurity, law enforcement, and personnel security components of the Army Insider Threat Program activities in order to provide commanders early warning of potential and emerging threats.
- d.* Ensure the coordination and synchronization of the Army Suitability Program, the Army Personnel Security Program, and the Army Insider Threat Program.

2–12. Deputy Chief of Staff, G–2

The DCS, G–2 will—

- a.* Serve as a member of the APPBOD and provide representation to the APPGOSC, APPCOC, and APPWG.
- b.* Serve as the APP lead for the Army Personnel Security Program, the Army Information Security Program, and the Industrial Security Program.
- c.* Serve as the proponent for personnel security, information security, industrial security, and foreign disclosure as they relate to or enable the APP and in coordination with the Army Special Programs Directorate, when applicable to SAP.
- d.* Develop and continuously maintain security measures to address gaps in the areas of personnel security, information security, industrial security, and intelligence/counterintelligence.
- e.* Recommend protection-related information and collection requirements to Army leaders in support of the APP.
- f.* Facilitate the sharing of intelligence, security, counterintelligence, and other related information with cybersecurity, law enforcement, and human resource components of the Army Insider Threat Program, to provide commanders early warning of potential and emerging threats.
- g.* Present annual strategic threat assessment report findings affecting APP primary and enabling functions to the APPBOD through the APP governance cycle to support APP synchronization and strategic-level decision-making, not later than the end of the second quarter of each fiscal year.
- h.* Coordinate and provide technical advice with regard to the development and implementation of Army protection and security policies.

2-13. Deputy Chief of Staff, G-3/5/7

The DCS, G-3/5/7 will—

- a.* Assist and support the ASA (M&RA) in developing and executing protection-related Army strategies, policies, and plans; executing and ensuring the execution of policies, plans, and programs by HQDA APPBOD board members and organizations; and reviewing and assessing the execution of policies, plans, and programs.
- b.* Organize, manage, and execute the APP as the HQDA staff lead and ensure HQDA APPBOD board members and commanders carry out their protection-related duties in a coordinated and integrated fashion.
- c.* Serve as the APP lead for Continuity of Operations (COOP), emergency management (EM), mission assurance (MA), insider threat (InT) and operations security (OPSEC).
- d.* Serve as a co-chair of the APPBOD. Designate the DCS, G-3/5/7 co-chair(s) for the APPGOSC, APPCOC and APPWG.
- e.* Support the HQDA APP Governance Cycle by providing an executive secretary to:
 - (1) Provide the entry point for referring issues to the APPBOD or any of its subcommittees, subgroups, and/or working groups.
 - (2) Provide daily and administrative support.
 - (3) Prepare and coordinate HQDA APP meetings (logistics, agendas, and minutes), as well as for the meetings and activities of subcommittees.
 - (4) Prepare and forward recommendations from the APPBOD to Army decision-makers or enterprise level management and/or resource bodies for review and guidance, as appropriate.
 - (5) Prepare and forward guidance, tasking, and/or data calls from the APPBOD to its subcommittees and track their input and/or responses.
 - (6) Coordinate all actions necessary to accomplish required APPBOD outputs and other tasks assigned by the APPBOD chairs.
 - (7) Ensure the APPBOD charter is updated and validated per AR 15-39.
 - (8) Ensure the work for the APPBOD is coordinated with other relevant Army enterprise-level bodies, Office of the Secretary of Defense, other Services, and Federal agencies, where appropriate.
- f.* Ensure the APP strategy and policy is appropriately linked with and nested under the DoD and JS protection-related programs.
- g.* Synchronize the exchange of protection information with the DoD, JS, and other Services to adopt best practices and improve protection policies and processes.
- h.* Ensure dissemination of DA level protection priorities and requirements to the Army commands (ACOMs), Army service component commands (ASCCs), DRUs, U.S. Army Reserve (USAR), and the Army National Guard (ARNG).
- i.* Develop and annually update the Army Prioritized Protection List (APPL) to identify and rank-order installations using an objective methodology that accounts for various factors including, but not limited to, standard garrison organization inputs, strategic functionality and criticality, and threat.
- j.* Serve as the APP “information hub” by providing the timely and accurate exchange of protection-related information and the formal and informal sharing of cross-programmatic issues, ideas, and best practices essential to the success of the APP. Coordinate for key APP information sharing capabilities by—
 - (1) Maintaining an APP online portal with appropriate information sharing, task tracking, and knowledge management tools to ensure maximum visibility of APP activities and support collaboration among APP components and increase visibility throughout the Army.
 - (2) Reviewing protection-related responses (for example, Congressional testimony, Government Accountability Office requests, and IG inspections) to highlight issues for potential briefing through the APP Governance Cycle.
 - (3) Coordinating with the DCS, G-9, and U.S. Army Training and Doctrine Command (TRADOC) to ensure orientation courses for senior commanders and garrison commanders include a list of strategic Army missions, assets, and capabilities for their respective commands.
 - (4) Integrating best practices within the broader protection community, including but not limited to, best practices from across DoD, JS, Department of Homeland Security, academia, and the private sector.
 - (5) Ensuring HQDA APP management framework priorities and recommendations are reflected in protection-related DA directives, regulations, pamphlets, orders, and messages.
 - (6) Publishing the Army Planning Priorities Guidance and APPL annually to senior commanders communicating strategic missions, assets, and capabilities.
- k.* Coordinate APP assessments (APPAs). Maintain a list of APPA benchmarks and make them available to the commands by a portal.

2-14. Deputy Chief of Staff, G-4

The DCS, G-4 will serve as a member of the APPBOD and provide representation to the APPGOSC, APPCOC, and APPWG.

2-15. Deputy Chief of Staff, G-6

The DCS, G-6 will—

- a.* Serve as the APP lead for Cybersecurity (CS) execution, implementation, and synchronization.
- b.* Facilitate sharing of AUAMP information.
- c.* In coordination with the DCS, G-2, synchronize and implement Army intelligence and automated information systems with the Army Insider Threat Program based on oversight and policy from HQDA CIO.
- d.* Support U.S. Army Cyber Command (ARCYBER) with subject matter expertise during the execution of CS function of protection, and its associated enabling functions.
- e.* In coordination with the DCS, G-2, oversee Army intelligence and automated information systems with the Army Insider Threat Program.
- f.* Serve as a member of the APPBOD and provide representation to the APPGOSC, APPCOC, and APPWG.

2-16. Deputy Chief of Staff, G-8

The DCS, G-8 will—

- a.* Serve as a member of the APPBOD and provide representation to the APPGOSC, APPCOC, and the APPWG.
- b.* Provide SME support to assist the DCS, G-3/5/7 in coordinating cross-MDEP and PEG integration and synchronization consistent with the APP and Army programming guidance. Assist the APP in planning, programming, budgeting and execution (PPBE) actions and Program Objective Memorandum (POM) development.
- c.* In coordination with DCS, G-3/5/7, DAMO – ODP (G-34), maintain a list of direct and indirect APP MDEPs and update the list annually.

2-17. Deputy Chief of Staff, G-9

The DCS, G-9 will—

- a.* Serve as a member of the APPBOD and provide representation to the APPGOSC, APPCOC, and APPWG.
- b.* Serve as the APP lead for the Fire and Emergency Services (F&ES).
- c.* Ensure the Installations Program Evaluation Group adequately addresses protection-related priorities throughout the PPBE process.
- d.* Provide access to manpower models and other protection-related data to the DCS, G-3/5/7, DAMO-ODP (G-34) from databases that support or impact protection-related services.
- e.* In coordination with the DCS, G-3/5/7, DAMO-ODP (G-34), develop and provide an integrated APP block of instruction at senior commanders, senior leaders, and garrison commander courses that includes a list of strategic Army missions, assets, and capabilities for their respective commands.
- f.* Assist the DCS, G-3/5/7 in planning, programming, and executing protection-related activities at Army installations and separate facilities.

2-18. Chief, National Guard Bureau

The CNGB will—

- a.* Serve as a member of the APPBOD and provide representation to the APPGOSC, APPCOC, and APPWG.
- b.* Publish guidance to all State Adjutants General concerning implementation of the APP and require them to publish state-specific guidance, including establishing Protection Executive Committees (PECs), developing emergency management and integrated protection plans (IPPs), and conducting consolidated and integrated protection exercises.
- c.* Execute the APP per chapter 5 of this regulation.

2-19. Chief of Army Reserve

The CAR will—

- a.* Serve as a member of the APPBOD and provide representation to the APPGOSC, APPCOC, and APPWG.
- b.* Publish guidance to subordinate commands concerning implementation of the APP, including establishing PECs, developing IPPs, and conducting consolidated and integrated protection exercises.
- c.* Execute the APP per chapter 5 of this regulation.

2–20. Chief of Engineers

The COE will serve as a member of the APPBOD and provide representation to the APPGOSC, APPCOC, and APPWG.

2–21. The Surgeon General

TSG will—

- a.* Serve as a member of the APPBOD and provide representation to the APPCOC, APPGOSC, and APPWG.
- b.* Serve as the APP lead for the Force Health Protection (FHP) function of protection and its associated enabling functions.
- c.* Ensure integration of protection considerations into FHP policy and contracting.

2–22. The Judge Advocate General

TJAG will serve as a member of the APPBOD and provide representation to the APPGOSC, APPCOC, and the APPWG.

2–23. Chief of Chaplains

The CCH will serve as a member of the APPBOD and provide representation to the APPGOSC, APPCOC, and APPWG.

2–24. The Provost Marshal General

The PMG will—

- a.* Serve as a member of the APPBOD.
- b.* Serve as a co-chair of the APPGOSC.
- c.* Designate an O–6 level (or equivalent) representative to co-chair the APPCOC.
- d.* Designate an O–5 level (or equivalent) representative to co-chair the APPWG.
- e.* Designate a liaison to the DCS, G–3/5/7, DAMO–ODP (G–34) for daily coordination of protection issues. This officer or civilian will perform daily duties inside the Office of the Provost Marshal General (OPMG). In a crisis that requires a standup of the Crisis Action Team, the PMG will provide a liaison to support the DCS, G–3/5/7, DAMO – ODP (G – 34).
- f.* Serve as the APP lead for the primary functions of antiterrorism (AT), law enforcement (LE), physical security (PS), and subordinate functions of high-risk personnel, Threat Information Fusion & Reporting (THREAT), and military working dogs.
- g.* Support the ASA (M&RA) and the DCS, G–3/5/7 in the execution of Army AT and protection efforts, including providing direct support for Antiterrorism Division and Army Threat Integration Center functions and supporting the ASA (IE&E) on installation PS.
- h.* Provide recommendations to the DCS, G–3/5/7 for inclusion in annual protection priorities.
- i.* Facilitate the sharing of law enforcement, criminal intelligence (CRIMINT), and other related information with cybersecurity, personnel security, counterintelligence, and human resource components of the Army Insider Threat Program to provide commanders early warning of potential and emerging threats.
- j.* Provide applicable Army Law Enforcement Compliance Program and Military Working Dog Program data annually to the DCS, G–3/5/7. Data provided will be used to augment the feedback received from the APPAs and to supplement reports addressing the trends and effectiveness of the APP.

2–25. Commanders of Army commands, Army service component commands, and direct reporting units

The commanders of ACOMs, ASCCs, and DRUs, will execute the APP per chapter 5 of this regulation.

2–26. Commanding General, U.S. Army Training and Doctrine Command

The CG, TRADOC will determine and submit APP-related doctrine and training requirements to the HQDA APPBOD for validation.

2–27. Commanding General, U.S. Army Cyber Command

The CG, ARCYBER will—

- a.* Coordinate with the DCS, G–6 for SME support during the execution of the CS function of protection, and its enabling functions.

b. Plan and execute the AUAMP capabilities of the Army's classified non-tactical computer networks, and facilitate sharing of AUAMP information with the Army Insider Threat Hub and the personnel security, counterintelligence, and law enforcement functions of the Army Insider Threat Program in order to provide commanders early warning of potential and emerging threats.

2–28. Director, U.S. Army Criminal Investigation Division

The Director, USACID will provide law enforcement and CRIMINT information, to the extent permitted by applicable law and regulation, to the Army Insider Threat Hub, a functional element of the Army Insider Threat Program, to enable the prevention, deterrence, detection, analysis, and response of insider threats.

2–29. Commanding General, U.S. Army Corps of Engineers

The CG, USACE will—

- a. Serve as the APP lead for the security engineering enabling function as it relates to and enables the APP.
- b. Coordinate Defense Sector Public Works outputs that impact the APP.
- c. Leverage USACE Centers of Expertise for best practices to support the APP enabling functions and make geographic information systems data available to support protection-related activities.
- d. Integrate protection considerations into public works projects as appropriate.

Chapter 3

The Army Protection Program

3–1. Army Protection Program functions

a. The APP enables the execution of Army missions in all threats and hazards environments by integrating, coordinating, synchronizing, and prioritizing the efforts and resources of the 19 APP functions with their associated programs and processes. Figure 3–1 shows the APP functions (primary, subordinate, and enabling).

b. The APP is comprised of the following primary, subordinate, and enabling functions:

(1) *Primary and subordinate functions.* The 13 primary functions and 3 subordinate functions of the APP are: Antiterrorism (AT) (includes subordinates: Threat Information Fusion & Reporting (THREAT), and high risk personnel), COOP, cybersecurity (CS), EM, Fire and Emergency Services (F&ES), Force Health Protection (FHP), law enforcement (LE) (includes subordinate: Military Working Dogs (MWDs), mission assurance (MA), Insider Threat (InT), OPSEC, physical security (PS), security programs (SP), and suitability (ST)).

(2) *Enabling functions.* The 3 enabling functions are: Intelligence, Counterintelligence, and Security Engineering.

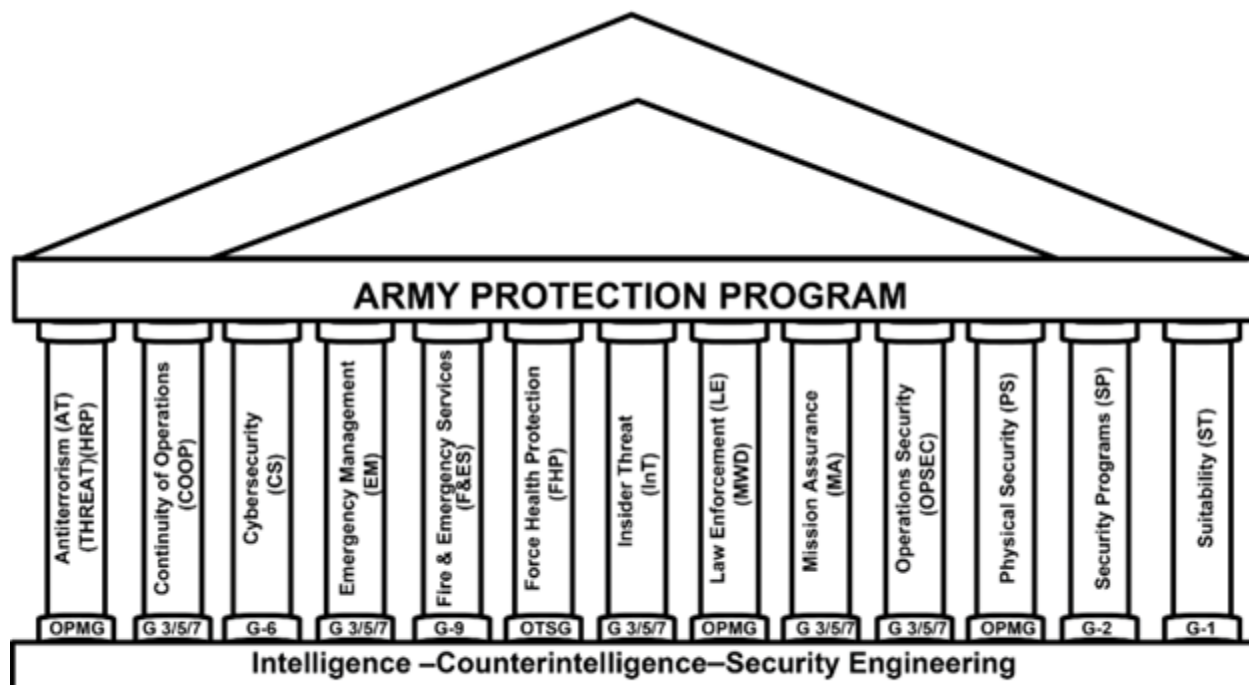


Figure 3–1. Army Protection Program's Functions

3–2. The Army Protection Program implementation

The APP unifies the Army protection efforts in order to support the execution of DoD and Army mission essential functions (MEFs). The APP cannot eliminate the risks of threats and hazards, but it does seek to prevent, prepare, protect, mitigate, respond, and recover from an event to minimize the impact on the execution of DoD and Army missions. Commanders at all levels will consider the following when managing the risk to DoD's and the Army's MEFs and other operational requirements:

a. Resilience, scalability, and sustainability. Effective protection activities minimize risks from all threats and hazards and strengthen the Army's ability to prepare for, prevent against, respond to, and recover from future incidents.

(1) *Resilience.* Protection activities increase resilience by reducing the impact and/or duration of disruptive events on missions, functions, and supporting assets and capabilities.

(2) *Scalability.* Protection policies, programs, plans, assessments, and training and exercises are scalable and flexible to meet current and emerging challenges.

(3) *Sustainability.* Protection efforts must be sustainable to meet both the current needs of commanders supporting on-going operations, while preparing for emerging threats and hazards. Layered, mutually supporting interoperable, and cyclical capabilities at all levels allow for sustained protection capabilities over time.

b. Risk-informed culture. A risk-informed culture supports protection activities. It relies on vigilance and situational awareness to support information sharing and risk-informed decision-making. Leaders are aware of the full spectrum of threats and prepare plans to effectively continue operational requirements.

(1) *Vigilance and situational awareness.* Vigilance—being continuously watchful and aware of threats and hazards—is the first step toward ensuring the safety and security of Soldiers, Civilians, Family members, contractors, facilities, infrastructure, and information. Situational awareness—a comprehensive understanding of current, evolving, and emerging threats and hazards and the relative risk they pose—forms the APP's common operational picture and serves as the strategic foundation of protection activities. Continuously assessing the threat picture allows the alignment of appropriate resources.

(2) *Information sharing and risk-informed decision-making.* Appropriate, accessible, and timely information allows for the ongoing analysis of risks and assessment of best practices. Risk-informed decision-making through the identification and prioritization of MEFs and supporting assets establishes priorities, helps focus operations on the most critical protection issues, and promotes sound investments. Appropriate risk information must be shared in order to share risk through the allocation of resources.

c. *Shared responsibility.* Protection is most effective as a shared responsibility within engaged partnerships working together through an integrated process. Installations provide common levels of support through programs such as LE, while commanders and Soldiers take appropriate actions to reduce risk.

(1) *Engaged partnerships.* The APP management framework provides a forum to exchange ideas, approaches, and best practices; facilitates security planning and resource allocation; establishes effective coordinating structures among partners; and builds unity of effort. Where possible, the APP shares information with and leverages best practices from the other Services, DoD and Army advisory boards, and Federal agencies.

(2) *Integrated process.* Working together across all levels of the Army, both horizontally and vertically, protection stakeholders can more effectively achieve a shared vision of a safe and secure Army that protects Soldiers, Civilians, Family members, contractors, facilities, infrastructure, and information.

(3) *Individual responsibility.* Protection is a multi-level endeavor requiring vigilance extending from the highest parts of the Army down to the individual Soldier. Protection is an Armywide responsibility with each individual doing their part to maintain situational awareness, report potentially dangerous situations, and develop skills to prepare for, protect against, respond to, and recover from a complex range of incidents.

d. *Transparency and accountability.* A transparent APP provides a more complete risk picture for senior leaders and promotes accountability at all levels.

(1) *Transparency.* Transparency helps enable the refinement of roles and responsibilities and improves understanding of interdependencies and evaluation of organizational effectiveness. The APP facilitates both formal and informal information sharing and serves as a repository of protection-related knowledge.

(2) *Accountability.* The APP expands program oversight, promotes leader accountability, and better facilitates informed decision-making and resource allocation.

e. *End-state focus.* The APP provides leaders and decision makers in each of the functions with actionable information based on consistent assessments and analyses.

(1) *Actionable information.* Assessments and analyses directly support mission-focused integrated protection decision-making and inform the PPBE process.

(2) *Consistent assessments.* Assessments employ documented metrics and use standards-based methods and processes.

(3) *Focused analysis.* Analysis leads to consistently developed courses of action that support the APP and Army MEFs.

f. *Forward looking.* Align the APP with the strategic goals of senior leadership, challenge long-held assumptions, and maintain flexibility to meet emerging threats and hazards. The APP seeks to integrate and coordinate protection processes in support of operational requirements, as opposed to executing a single policy or program by—

(1) Coordinating across protection functions and creating a more complete and accurate understanding of risks.

(2) Enabling senior leaders to address systemic risks and trends through integrated and synchronized protection policies, plans, programs, and resources.

(3) Coordinating protection and resilience requirements between mission owners and asset owners.

(4) Identifying dependencies outside of Army control and facilitating relationships with Federal, State, local government, private-sector, and international partners.

3–3. Army Protection Program Governance Cycle, at Headquarters Department of the Army

The APP governance cycle provides an enterprise approach to integrate, coordinate, synchronize, and prioritize APP initiatives and resources. It provides oversight, leadership, and governance by addressing non-warfighting protection-related issues at the lowest possible level.

a. The HQDA APP governance cycle consists of APPBOD, APPGOSC, APPCOC, APPWG and associated working groups, as required, and as further described in appendix C. At the HQDA level, the APP expands program oversight, ensures senior leader accountability, and facilitates informed decision making and resource allocation (see para 4–2).

b. The PEC is the APP management framework at commands, installations, and stand-alone facilities that leverages APP principles and best practices to coordinate, integrate, synchronize, and prioritize resources with a unity of effort across the APP primary and enabling functions.

Chapter 4

Headquarters, Department of the Army

4-1. Army Protection Program activities at Headquarters, Department of the Army

The HQDA APPBOD board members develop, integrate, and synchronize protection policies, plans, programs, and resources to proactively link strategic risk management decisions to operational requirements and critical functionality. HQDA APPBOD board members coordinate Army priorities in concert with the Geographic Combatant Commanders' theater priorities.

- a. HQDA APPBOD board members will—
 - (1) Evaluate Armywide risk by reviewing trends analysis, discussing strategic protection and resiliency issues, and advocating acceptance, mitigation, or resolution of risk.
 - (2) Provide input to The Army Plan (TAP) and other strategic guidance.
 - (3) Inform senior leaders.
 - (4) Review and approve the APPL annually to identify and rank-order installations using an objective methodology that accounts for various factors including, but not limited to, standard garrison organization inputs, strategic functionality and criticality, and threat.
 - (5) Coordinate internally and with external partners, including but not limited to:
 - a. JS, DoD, combatant commands, and Army senior committees and boards (for example, Services and infrastructure core enterprise).
 - b. Joint program executive offices (JPEOs) (for example, JPEO Chemical, Biological, Radiological and Nuclear Defense).
 - c. Federal, State, and local agencies.
 - d. Private sector critical infrastructure owners, operators, and service providers.
 - e. Host nations, allies, and other mission partners.
- b. The HQDA APPBOD board members identified in chapter 2 who manage and execute the primary functions of the APP and the associated enabling functions as described in appendix B will—
 - (1) Manage and execute the protection program(s) for which they are the responsible proponent within the APP framework.
 - (2) Members of the Secretariat coordinate key decisions and policies prior to publication; members of the ARSTAF coordinate issues and concerns prior to implementation and execution. Coordinate key protection related decisions, issues, policies, and concerns with the APPBOD co-chairs (the DCS, G-3/5/7 and the ASA M&RA) APPBOD board of directors prior to implementation, publication, or execution.
 - (3) Identify program priorities, emerging issues, and other protection-related topics for inclusion in the TAP and other strategic documents through the HQDA APP Governance Cycle.

4-2. Planning, Programming, Budgeting, and Execution cycle

This regulation does not change current functional proponentcy for MDEPS. The APPBOD's executive secretary within the DCS, G-3/5/7, DAMO-ODP (G-34) will work with the principal chairs of the Planning, Programming, Budgeting Committee (PPBC) (DCS, G-3/5/7; DCS, G-8; and Director, Army Budget and PEG executives) during all phases of the PPBE cycle. The HQDA APP Governance Cycle leverages the PPBE process to maintain relevant funding levels to address Army priorities and current and emerging threats and hazards. At the direction of the APPBOD the DCS, G-3/5/7 advocates for protection resources and serves as an arbitrator among the protection programs across the following PPBE phases:

- a. *Planning.* The DCS, G-3/5/7 coordinates with the principal leads for each section of TAP to ensure protection-related equities are appropriately addressed. Through the HQDA APP Governance Cycle, the DCS G-3/5/7 develops feedback for overarching strategic guidance for inclusion in TAP, as well as specific guidance on enterprise solutions for MDEP managers to align APP priorities with DoD and Army senior leader priorities.
- b. *Programming.* Through the HQDA APP Governance Cycle, the DCS, G-3/5/7 develops enterprise wide solutions of protection-related issues, and forwards to the appropriate MDEP to ensure APP equities are adequately addressed in the POM process HQDA APP management framework develops overarching protection-related programming guidance based on APPBOD and other senior leader priorities.
- c. *Budgeting.* In coordination with the HQDA APPBOD, MDEP managers of APP supporting MDEPs will—
 - (1) Support protection priorities in accordance with APPBOD guidance and priorities.
 - (2) Attend PPBC meetings involving protection-related issues when directed.
 - (3) Participate in MDEP briefs to respective PEG for each direct MDEP and indirect MDEPs, as needed.
 - (4) Attend PPBC meetings involving protection-related issues.

(5) Coordinate with ASA (FM&C) budget integration and formulation, impacted commands, and programs during the Program Budget Review cycle for protection related resource requirements.

(6) Coordinate with DCS, G-3/5/7 Congressional Affairs Contact Officer and ASA (FM&C) to ensure proper visibility and response to all protection-related funding inquiries.

d. Execution. The APPBOD through the DCS, G-3/5/7 will provide guidance, feedback, and decision-making process involving protection-related issues.

4-3. Army Protection Program assessments

a. The DCS, G-3/5/7, DAMO-ODP (G-34) in coordination with HQDA SMEs from the APP primary functions and their associated enabling functions, will conduct triennial assessments of ACOMs, ASCCs, DRUs, and the ARNG. Where appropriate, the APPAs will coordinate with other DoD, JS, and other Army assessment teams (for example, IG, Army Audit Agency, Army Safety Office).

b. The APPAs measure the command's implementation and execution of the APP processes, and overall compliance with APP-related regulatory guidance. HQDA SMEs brief the results of the APPAs at the appropriate classification level to inform senior leaders and facilitate the efficient and effective PPBE of protection-related resources throughout the Army.

c. The DCS, G-3/5/7, DAMO-ODP (G-34) will—

(1) Maintain a list of assessment benchmarks updated annually and share them with stakeholders through the APP portal site.

(2) Publish an annual execution order outlining the APPA schedule, frequency, benchmarks, and pre-coordination responsibilities for the fiscal year.

(3) Approve special assessment areas for APPAs.

(4) Provide staff assistance visits to guide in the development and implementation of integrated protection plans at the command's request.

(5) Lead the HQDA semi-annual observation resolution boards to track corrective actions from APPAs and associated reply by endorsements (RBEs).

(6) Publish an annual APPA trend report that encompasses the current fiscal year APPA results focusing on benchmark deficiencies, reoccurring deficiencies, and best practices. This report should be used to sustain or increase protection readiness for all units. In order to capture trends over time this report primarily analyzes trends for the current FY and data from past assessments.

Chapter 5

Commands, Agencies, Activities, and Installations

The APP enables commands, installations, and standalone facilities to nest their protection programs and efforts with HQDA and Army strategic priorities. Commands, installations, and stand-alone facilities execute the APP to ensure that tactical and operational vulnerabilities do not compromise strategic and operational capabilities. Commanders of ACOMs, ASCCs, and DRUs; the CNGB; and senior leaders of agencies and activities will implement the APP through: planning and integration; training; exercise integration; assessing; and evaluating.

5-1. Planning and integration

Commanders of ACOMs, ASCCs, and DRUs; the CNGB; and senior leaders of agencies and activities will—

a. Identify and prioritize critical MEFs, other operational requirements, and critical assets through mission analysis to focus APP priorities and resources.

b. Issue APP guidance to subordinate commands and organizations to establish priorities and fully implement the requirements of this regulation to ensure the command's protection requirements are coordinated with supporting commands, and down to the installation(s) and/or stand-alone facilities where they reside. The APP guidance may include which subordinate commands and organizations will establish their own PECs, develop IPPs as per appendix D, exercise requirements and priorities, or be included in the higher headquarters PEC and IPP.

c. Ensure protection-related programs are assessed as part of the command's organizational inspection program (OIP), and that protection assessments complement rather than duplicate each other.

d. Within the command's operations or similar organization, synchronize, integrate, and coordinate the APP primary functions and the associated enabling functions to focus protection efforts on the command's, the Army's, and DoD's MEFs, other operational requirements, infrastructure, information, and security of personnel.

e. Facilitate the integration, coordination, and synchronization of APP efforts through the following organizations:

(1) The PEC reviews protection related initiatives. The PEC includes and encompasses all other protection-related executive councils and approval authority boards, and should meet a minimum of twice a year. The commander or their designee will chair the PEC and make all final decisions based on risk analysis for the utilization of resources to correct or mitigate vulnerabilities, and document decisions to accept risk.

(2) The Protection Working Group (PWG) is the body of action officers from each protection function that develops plans and exercises, conducts assessments, and makes suggestions and/or recommendations to the PEC on the means and methods to ensure execution of DoD and Army missions, and the security of the force. When possible, consolidate working groups for efficiencies while meeting the intent and requirements of individual protection-related regulations (for example, OPSEC Working Group, AT Working Group, EM Working Group, AT Threat Working Group, and PS Council). The PWG develops the command's IPP for the PEC and commander as per appendix D. Protection-related working groups should present issues through the PEC to ensure the synchronization of protection efforts. The PWG should meet at least twice a year.

(3) The Protection Threat Working Group (PTWG) is responsible for addressing and assessing threats and hazards that could impact the command. It will prepare recommendations for the protection working groups and the PEC. The PTWG must appropriately consider classification of products and discussion when sharing with associated non-Government personnel. The PTWG should meet at least quarterly and as required whenever there are changes in threats and/or hazards.

f. Through the command's PEC and working groups, commanders will—

(1) Evaluate command-wide risk by reviewing trend analysis, discussing strategic protection and resiliency issues, and advocating resolution, mitigation, or acceptance of risk.

(2) Participate in semi-annual observation resolution boards, chaired by DAMO-ODP (G-34), to track corrective actions from APPAs and associated RBEs.

(3) Ensure subordinate commands' and organizations' protection requirements are coordinated with supporting commands, down to the installation(s) and/or stand-alone facility where they reside.

(4) Prioritize risk management actions and mitigations at the command to eliminate unnecessary redundancies, achieve closer integration of APP activities, and improve application resources and future investments.

(5) Develop IPP per appendix D to address the continued execution of MEFs, other operational requirements, protection of critical assets, and security of personnel as determined by mission analysis and identified by higher headquarters, including the APPL. Address how the command will prepare for, prevent against, respond to, and recover from all threats and hazards. Share relevant sections of IPPs with senior commanders and leaders at applicable installations and stand-alone facilities so they can be supported by Installation Emergency Management Plans. The IPP and other protection-related plans will be developed and synchronized through the PWG and PEC, updated triennially, and approved by the commander or senior leader.

(6) Protection-related working groups will review subordinate commands' IPPs and other protection-related plans at least annually to ensure compliance with higher headquarter guidance and priorities. The working groups will assist subordinate commands in coordinating and resolving protection-related challenges.

(7) Coordinate APP requirements with external partners, including but not limited to: State and local agencies; host nations, allies, and other mission partners; and Non-Governmental Organizations (NGOs).

(8) Manage risk through shared responsibility with both internal and external partners.

(9) Continuously assess activities in operational environments to ensure threats and vulnerabilities are identified, risk management decisions are made, and appropriate measures are applied across the APP functions to ensure mission accomplishment.

(10) Inform the Army Operations Center (AOC) at HQDA, and the applicable ASCC(s), through the chain of command, at the appropriate level of classification, of any identified risks to Army and DoD strategic capabilities that is not within the purview of the command to resolve or mitigate. Ensure the DCS, G-3/5/7, DAMO-ODP (G-34) is aware of any protection related issue submitted to the AOC, and that is beyond the ability of a command to resolve internally.

g. Commanders at installations and/or stand-alone facilities have the best understanding of their local, site-specific circumstances to make decisions regarding the allocation of protection-related resources at their installations and stand-alone facilities. Commanders at installations and/or stand-alone facilities, in addition to the above, will—

(1) Chair the installation and/or stand-alone facility PEC with membership including the facility/garrison commander, staff principals representing the APP Functions, tenant commands, and other representatives as designated by the chair. Consider tenant organizations' requirements and include them in protection-related working groups.

(2) Facilitate risk management dialogues by bringing together operational, support, and tenant units to better understand and collaboratively manage shared risk.

(3) Integrate and leverage resource investments across the APP functions.

- (4) Promote information sharing and unity of effort among APP functions and tenant organizations.
- (5) Ensure all organic (such as, engineer, medical, LE, and PS) and tenant protection plans are incorporated into the overall installation protection plans.
- (6) Evaluate command, installation, and/or stand-alone facility-wide risk by reviewing trend analysis, discussing strategic protection and resiliency issues, and advocating acceptance, mitigation, or resolution of risk.
- (7) Develop protection-related guidance and standards to address Army installation and facility access.
- (8) Establish and maintain support agreements, including Mutual Aid Agreement (MAA), memorandum of understanding (MOU), memorandum of agreement (MOA), Inter-Service Support Agreement (ISSA), and support contracts for coordinated response and recovery support with civil and military partners, including coordination with local governments, first responders, NGOs, and the private sector critical infrastructure owners, operators, and service providers (where applicable).
- (9) Ensure appropriate protection-related measures are incorporated into the contract process and vendor activities.
- (10) Ensure IPPs and supporting plans support HQDA priorities, MEFs and tenant and supported commands, agencies, and activities through all stages of events.
- (11) Establish and convene a PWG, PTWG and develop an IPP.

5-2. Training

Commanders provide integrated APP functional training guidance to subordinate and tenant commands. APP function protection-related training guidance will be integrated into commanders' annual training guidance to subordinate and tenant commands. Unit commanders will integrate protection into unit training exercises. Protection-related requirements of the enabling functions will be identified and integrated into installation and facility annual training plans. Coordinate with external partners for their participation in appropriate protection training.

5-3. Exercise integration

a. Commanders will ensure their commands develop a progressive, multi-year exercise program that enables subordinates to participate in a series of increasingly complex, risk-informed capabilities-based exercises, with each linked to a set of common protection priorities designed to test associated capabilities. Exercise programs will follow Homeland Security Exercise and Evaluation Program principles and will progress from seminars to drills to tabletop exercises to functional exercises to a full-scale exercise (FSE). Exercises will operate within the progressive series guidelines, and will address all individual APP functions at least once every three years. All requirements set forth in primary functions regulations will be completed within their prescribed timeframes, but should support multi-year exercise plans culminating in an all-hazards FSE in accordance with AR 525-27.

b. Triennially: The senior commander will conduct an all-hazards externally evaluated FSE that integrates multiple agencies, multiple jurisdictions, and all protection functions based on risks from identified hazards and threats, including incidents with cascading impacts. Capabilities from all the APP functions and command and control capabilities within the command's sphere of control and influence, must be included in a full-scale protection exercise over a three year period, but it is not mandated that all functions have to be addressed in one event. Senior commanders will ensure their installations develop a progressive, multi-year exercise program that enables subordinates to participate in a series of increasingly complex, risk-informed capabilities-based exercises, with each linked to a set of common protection priorities designed to test associated capabilities. Each exercise within the progressive series will follow Homeland Security Exercise and Evaluation Program guidelines, and will address all individual APP Functions at least once every three years.

c. Commanders will coordinate with external partners for appropriate participation in integrated protection exercises per existing MAAs, MOUs, MOAs, and ISSAs for both response and consequence management phases.

d. Commanders may forgo exercising specific APP functions if they were executed in support of a real world event (for example, response to a tornado or hurricane). Real world events that test the APP functions must be captured in an after-action report and corrective actions implemented in order to receive exercise credit.

e. Commanders will provide an after-action report at the applicable classification level of each full-scale protection exercise with lessons learned to the higher headquarters. After-action reports of full-scale protection exercises will be maintained for a minimum of 4 years.

5-4. Assessing

Commanders will self-assess their protection related programs as part of their OIP and assess subordinate commands to ensure proper execution and overall compliance with the APP-related protection programs. They will also evaluate the command's training and exercise programs, the risk management decision processes, and identify trends and best practices.

a. Use SMEs from the APP functions and the associated enabling functions to conduct tailored and integrated assessments of their subordinate commands, a minimum of triennially, using the APP assessment benchmarks maintained by the DCS, G-3/5/7, DAMO-ODP (G-34) at the designated portal (<https://intelshare.intelink.gov/sites/hqdag34/protection/appa/documents/forms/allitems.aspx>). Any other standards used for protection assessments must be HQDA-vetted and approved. Integrate the assessment of specific protection programs requirements as prescribed by the applicable regulations.

b. Publish an annual assessment schedule of subordinate commands. Minimize the number of assessments of subordinate commands by scheduling and combining assessments with other DoD, JS, and Army assessment teams (IG, HQDA APPAs, Army Audit Agency, and Army Safety Office) whenever possible. When appropriate, Commanders may use external assessments to meet higher headquarters' assessment requirements. ACOM, ASCC, and DRU commanders will inform the DCS, G-3/5/7, DAMO-ODP (G-34) of pending assessments by external DoD and Federal organizations.

c. Within 90 days of the completion of an assessment of any of the APP functions, prioritize and/or track identified discrepancies and/or vulnerabilities, and develop a plan of action to mitigate or eliminate the discrepancies and/or vulnerabilities. Track corrective actions from APPAs and associated assessments' and RBEs. Assessments are not considered final until discrepancies and/or vulnerabilities have been adjudicated by the command.

5-5. Evaluating

a. Commanders will evaluate all APP primary functions every three years to determine the effectiveness of the guidance provided, processes, effectiveness of training and exercises conducted, involvement of external partners, overall compliance with APP-related regulatory guidance, identify trends, determine new requirements, review APP best practices, and determine the priorities for the development of the annual protection training plan and exercise program for the following year.

b. Identify APP best practices and recommend solutions to improve protection risk management and build resiliency at the command or installation level.

c. Commanders can request Staff Assistance Visits for select APP areas from HQDA through the DCS, G-3/5/7, DAMO-ODP (G-34) to assist in the implementation of APP (PEC, Critical Asset Identification Process, IPPs, assessment benchmarks, and expertise) at the command's request.

Appendix A

References

Section I

Required Publications

This section contains no entries.

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. Army publications are available on the Army Publishing Directorate website at <https://armypubs.army.mil>; DoD publications are available at <https://www.esd.whs.mil>; Chairman of the Joint Chiefs of Staff and Joint publications are available at <https://www.jcs.mil/library>.

AD 2013–18

Army Insider Threat Program

ADP 3–37

Protection

ADP 4–0

Sustainment

AR 1–201

Army Inspection Policy

AR 5–22

The Army Force Modernization Proponent System

AR 10–87

Army Commands, Army Service Component Commands, and Direct Reporting Units

AR 11–2

Managers' Internal Control Program

AR 15–39

Department of the Army Intergovernmental and Intragovernmental Committee Management Program

AR 20–1

Inspector General Activities and Procedures

AR 25–1

Army Information Technology

AR 25–2

Army Cybersecurity

AR 25–22

The Army Privacy and Civil Liberties Program

AR 25–30

Army Publishing Program

AR 25–55

The Department of the Army Freedom of Information Act Program

AR 40–5

Army Public Health Program

AR 40–501

Standards of Medical Fitness

AR 40–562

Immunizations and Chemoprophylaxis for the Prevention of Infectious Diseases

AR 70-1

Army Acquisition Policy

AR 190-5

Motor Vehicle Traffic Supervision

AR 190-9

Absentee Deserter Apprehension Program and Surrender of Military Personnel to Civilian Law Enforcement Agencies

AR 190-11

Physical Security of Arms, Ammunition, and Explosives

AR 190-12

Military Working Dog Programs

AR 190-13

The Army Physical Security Program

AR 190-14

Carrying of Firearms and Use of Force for Law Enforcement and Security Duties

AR 190-17

Biological Select Agents and Toxins Security Program

AR 190-24

Armed Forces Disciplinary Control Boards and Off-Installation Liaison and Operations

AR 190-30

Military Police Investigations

AR 190-45

Law Enforcement Reporting

AR 190-47

The Army Corrections System

AR 190-51

Security of Unclassified Army Resources (Sensitive and Non-sensitive)

AR 190-54

Security of Nuclear Reactors and Special Nuclear Materials

AR 190-55

U.S. Army Corrections System: Procedures for Military Executions

AR 190-56

The Army Civilian Police and Security Guard Program

AR 190-58

Designation and Protection of High Risk Personnel

AR 190-59

Chemical Agent Security Program

AR 195-2

Criminal Investigation Activities

AR 195-5

Evidence Procedures

AR 380-5

Army Information Security Program

AR 380-10

Foreign Disclosure and Contacts with Foreign Representatives

AR 380-27

Control of Compromising Emanations

AR 380–28
Army Sensitive Compartmented Information Security Program

AR 380–40
Safeguarding and Controlling Communications Security Material

AR 380–49
Industrial Security Program

AR 380–53
Communications Security Monitoring

AR 380–67
Personnel Security Program

AR 380–381
Special Access Programs (SAPs) and Sensitive Activities

AR 381–10
The Conduct and Oversight of U.S. Army Intelligence Activities

AR 381–12
Threat Awareness and Reporting Program

AR 420–1
Army Facilities Management

AR 500–3
U.S. Army Continuity of Operations Program

AR 525–13
Antiterrorism

AR 525–26
Infrastructure Risk Management (Army)

AR 525–27
Army Emergency Management Program

AR 530–1
Operations Security

AR 600–20
Army Command Policy

AR 600–63
Army Health Promotion

AR 600–78
Army Suitability Program

AR 630–10
Absence Without Leave, Desertion, and Administration of Personnel Involved in Civilian Court Proceedings

ATP 3–39.20
Police Intelligence Operations

ATP 3–39.32
Physical Security

CJCSI 6211.02D
Defense Information Systems Network (DISN) Responsibilities

CJCSI 6510.01F
Information Assurance (IA) and Support to Computer Network Defense (CND)

DA Pam 25–403
Army Guide to Recordkeeping

DA Pam 40–11

Army Public Health Program

DA Pam 385–30

Risk Management

DA Pam 525–27

Army Emergency Management Program

DA Pam 600–24

Health Promotion, Risk Reduction, and Suicide Prevention

DoD 5240.1–R

Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons

DoDD 3020.26

DoD Continuity Policy

DoDD 3020.40

Mission Assurance (MA)

DoDD 5200.27

Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense

DoDD 5205.02E

DoD Operations Security (OPSEC) Program

DoDD 5205.16

The DoD Insider Threat Program

DoDD 5230.11

Disclosure of Classified Military Information to Foreign Governments and International Organizations

DoDD 5240.01

DoD Intelligence Activities

DoDD 5525.04

Enforcement of the State Traffic Laws on DoD Installations

DoDD 6200.04

Force Health Protection (FHP)

DoDD 6490.02E

Comprehensive Health Surveillance

DoDI 2000.12

DoD Antiterrorism (AT) Program

DoDI 3020.42

Defense Continuity Plan Development

DoDI 3020.45

Mission Assurance Construct

DoDI 3020.52

DoD Installation Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive (CBRNE) Preparedness Standards

DoDI 5200.08

Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB)

DoDI 5200.46

DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC)

DoDI 5200.48

Controlled Unclassified Information (CUI)

DoDI 5210.65

Security Standards for Safeguarding DoD Chemical Agents

DoDI 5240.04

Counterintelligence (CI) Investigations

DoDI 5400.11

DoD Privacy and Civil Liberties Programs

DoDI 5525.09

Compliance with Court Orders by Service Members and DoD Civilian Employees, and Their Family Members Outside the United States

DoDI 5525.15

Law Enforcement (LE) Standards and Training in the DoD

DoDI 6055.06

DoD Fire and Emergency Services (F&ES) Program

DoDI 6055.17

DoD Emergency Management (EM) Program

DoDI 6200.03

Public Health Emergency Management (PHEM) within the DoD

DoDI 6490.03

Deployment Health

DoDI 8500.01

Cybersecurity

DoDI O–2000.16, Volume 1

DoD Antiterrorism Program Implementation: DoD Antiterrorism Standards

DoDM 5100.76

Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives (AA&E)

DoDM 5200.01, Volume 1

DoD Information Security Program: Overview, Classification, and Declassification

DoDM 5200.01, Volume 2

DoD Information Security Program: Marking of Information

DoDM 5200.01, Volume 3

DoD Information Security Program: Protection of Classified Information

DoDM 5205.02

DoD Operations Security (OPSEC) Program Manual

EO 13587

Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding Classified Information

FM 4–02

Army Health System

Homeland Security Presidential Directive 12

Policy for a Common Identification Standard for Federal Employees and Contractors (Available at <https://www.dhs.gov/homeland-security-presidential-directive-12>.)

JP 1

Doctrine for the Armed Forces of the United States

JP 1–02

DoD Dictionary of Military and Associated Terms

JP 3–0

Joint Operations

JP 3–07

Stability

JP 3–10

Joint Security Operations in Theater

JP 3–13

Information Operations

JP 3–33

Joint Task Force Headquarters

JP 3–34

Joint Engineer Operations

JP 5–0

Joint Planning

Presidential Memorandum–National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs

(Available at <https://www.whitehouse.gov/the-press-office/2012/11/21/presidential-memorandum-national-insider-threat-policy-and-minimum-stand->)

Public Law 108–458

Intelligence Reform and Terrorism Prevention Act of 2004 (Available at <https://www.gpo.gov/fdsys/search/home.action>.)

Public Law 110–53

Implementing Recommendations of the 9/11 Commission Act of 2007 (Available at <https://www.gpo.gov/fdsys/search/home.action>.)

5 CFR 731

Suitability

5 CFR 731.203

Suitability actions by OPM and other agencies

10 USC 7013

Secretary of the Army (Available at <https://www.gpo.gov/fdsys/search/home.action>.)

50 USC 797

Penalty for violation of security regulations and orders (Available at <https://uscode.house.gov>.)

Section III**Prescribed Forms**

This section contains no entries.

Section IV**Referenced Forms**

Unless otherwise indicated, DA forms are available on the APD website at <https://armypubs.army.mil>.

DA Form 11–2

Internal Control Evaluation Certification

DA Form 2028

Recommended Changes to Publications and Blank Forms

Appendix B

The Army Protection Program Functions

B-1. Army Protection Program primary functions

This section briefly identifies the APP primary functions, the supporting HQDA principal official, and the primary references for that function. Additional references are found in appendix A.

a. Antiterrorism.

(1) *General.* AT is defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military and civilian forces. The AT Program is a collective, proactive effort focused on the prevention and detection of terrorist attacks against DoD personnel, their families, facilities, installations, and infrastructure critical to mission accomplishment, and the preparation to defend against and planning for the response to the consequences of terrorist incidents. Commanders of ACOMs, ASCCs, and DRUs; and the CAR and the CNGB are responsible for incorporating AT into their plans and operations. AT program includes Threat Information Fusion & Reporting and High Risk Personnel.

(2) *Army principal official.* The PMG supports the HQDA, DCS, G-3/5/7 for the management and execution of the Army AT mission.

(3) *Primary reference.* AR 525-13, AR 190-58.

(4) *Supporting references.* ATP 3-37.2, DoDI 2000.12, DoDI O-2000.16, and JP 3-07.2.

b. Continuity of Operations Program.

(1) *General.* COOP is policies, plans, procedures, and capabilities that provide for the continued execution of mission essential functions across a wide range of potential emergencies, including localized acts of nature, accidents, technological, and/or attack related emergencies. The COOP responsibilities include developing and maintaining a COOP program and maintaining a COOP operations plan that identifies and prioritizes MEFs.

(2) *Army proponent.* The DCS, G-3/5/7 is the proponent for COOP.

(3) *Primary reference.* AR 500-3.

(4) *Supporting references.* DoDD 3020.26, and DoDI 3020.42.

c. Cybersecurity.

(1) *General.* Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

(2) *Army proponent.* The Army Chief Information Officer.

(3) *Primary reference.* AR 25-2.

(4) *Supporting references.* AR 25-1, AR 195-2, AR 380-5, AR 380-53, AR 380-381, Chairman of the Joint Chiefs of Staff Manual 6510.01B, DoDI 8500.01, and DoDI 8510.01.

d. Emergency management.

(1) *General.* The EM function serves as the single, comprehensive, and integrated EM program on Army installations, facilities, activities and associated off-installation areas (stand-alone facilities) subject to Army jurisdiction. The Army EM Program is responsible for all activities and operations related to preparing for, mitigating the potential effects of, preventing, responding to, and recovering from all multi-agency and/or multijurisdictional emergencies on or impacting Army installations worldwide. The Army EM Program functions within an all hazards environment consisting of all natural, technological, and human-caused hazards, including terrorism threats or incidents. The EM function includes the implementation of EM program training, standards, and National Incident Management System procedures; all-hazard preparedness; and ensuring Army installations comply with EM requirements, participate in the EM planning process, and provide personnel support as specified in host installation EM Plans.

(2) *Army proponent.* The DCS, G-3/5/7 is the proponent for the Army EM Program.

(3) *Primary reference.* AR 525-27.

(4) *Supporting references.* AR 600-20, DA Pam 525-27, DODI 3020.52, and DODI 6055.17.

e. Fire and Emergency Services.

(1) *General.* F&ES is the program that ensures public safety by providing response capabilities and medical services during emergencies. The F&ES Program assists in suggesting policy formulation, strategy development, enterprise integration, program analysis and integration, requirements and resource determination, and best business practices for services, programs, and installation support to Soldiers, Civilians, Family members, and to an expeditionary Army.

(2) *Army principal official.* The DCS, G-9 supervises execution of the F&ES Program.

(3) *Primary reference.* AR 420-1.

(4) *Supporting reference.* DoDI 6055.06.

f. Force Health Protection.

(1) *General.* FHP consists of programs and processes that promote and sustain a healthy and fit force, prevent injury and illness, and protect the force from health hazards, resulting in Army mission accomplishment and protection of the Army Family across the full range of military activities and operations. FHP includes: medical emergency readiness (preparedness, response, and special teams); health promotion (Soldier medical readiness, health education, and community resilience); occupational and environmental health (OEH) surveillance (identification of health hazards, assessing potential exposures, and collection/archival of ALL OEH data); medical interventions (immunizations, preventive therapies, and medical countermeasures); medical intelligence (medical information, global health engagements, and medical analysis); and medical surveillance (analysis, interpretation, and reporting of: instances of disease and injury, medical interventions, stress-induced casualties, combat casualties, and medical evacuations). FHP constitutes medical and public health activities and measures that identify, prepare for, and respond to health hazards and emergencies, resulting in Army mission accomplishment and protection of the Army Family. FHP includes: medical emergency readiness (preparedness, response, and special teams); health promotion (risk communication, occupational health, and community resilience); medical therapeutics (for emerging and continental United States threats and distribution capability); medical prophylaxis (vaccines, pretreatments, and protective measures); medical intelligence (medical information, global health engagements, and medical analysis); and medical surveillance (risk, reports, and impact on the force).

(2) *Army principal official.* TSG provides technical advice and assistance for FHP.

(3) *Primary references.* AR 40–5 and DoDI 6200.03.

(4) *Supporting references.* AR 40–501, AR 40–562, AR 525–27, AR 600–63, DA Pam 40–11, DA Pam 600–24, Army Doctrine Reference Publication (ADP 4–0), FM 4–02, DoDD 6490.02E, DoDD 6200.04, and DoDI 6490.03.

g. Insider Threat Program.

(1) *General.* The Army Insider Threat Program is an integrated HQDA effort to prevent, deter, detect, and mitigate risk posed by “insiders,” who may damage the security of the United States. The Army Insider Threat Program ensures adherence to Army insider threat policy and maintains a counter insider threat mission to comply with requirements and standards established to prevent, deter, detect, and mitigate the threat insiders can pose to the Army, the DoD, and U.S. Government installations, facilities, personnel, missions, or resources. This threat can include damage to the U.S. through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental capabilities or resources (including personnel, assets, and facilities).

(2) *Army proponent.* The DCS G–3/5/7 is the proponent for the Army Insider Threat Program.

(3) *Primary references.* AD 2013–18; DoDD 5205.16 and EO 13587.

(4) *Supporting references.* Presidential Memorandum–National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs.

h. Law enforcement.

(1) *General.* LE is directing, developing, and monitoring implementation of HQDA policies pertaining to LE, military working dogs, police intelligence, military police investigations, military police offense reporting, U.S. Army Deserter Information Program, and other provost marshal activities.

(2) *Criminal intelligence.* CRIMINT incorporates criminal investigations, forensic science examinations, biometric identifications, and protective service operations into protection. CRIMINT efforts contribute to protection of the force by conducting collection, analysis, investigations, and operations designed to identify domestic terrorist and extremist activities, as well as criminal activities that threaten the survivability and mission accomplishment of military personnel, civilian employees, Family members, contractors, and units.

(3) *Army principal official.* The PMG assists in the development of policies and procedures for Army LE.

(4) *Primary references.* AR 190–30 and AR 190–45.

(5) *Supporting references.* AR 190–5, AR 190–9, AR 190–11, 190–12, AR 190–13, AR 190–14, AR 190–24, AR 190–47, AR 190–55, AR 190–56, AR 195–2, AR 195–5, AR 630–10, ATP 3–39.20, DoDD 5525.04, DoDI 5200.08, DoDI 5240.04, DoDI 5525.09, and DoDI 5525.15.

i. Mission assurance.

(1) *General.* MA is the Army program which implements the Mission Assurance requirements in accordance with DoDD 3020.40 and DODI 3020.45. The MA construct’s four processes are identification, assessment, risk management, and reporting and monitoring. The Army MA program focuses on Army-owned or operated task critical assets (TCA) categorized as Tier 1 (TCA–1) and Tier 2 (TCA–2), and on coordination with sister-services and Defense Agencies to protect non-Army owned TCAs on Army installations. The DCS, G–3/5/7 executes a triennial identification and annual validation of these TCAs. The DCS, G–3/5/7 executes periodic Mission Assurance Assessments at these locations that link the assets’ vulnerabilities to those threats and hazards likely to impact the asset in order to

discover the risks to mission. The DCS, G-3/5/7 works with commands to develop risk reduction plans for their assets and then advocates for risk mitigation actions with HQDA, the Joint Staff and the Office of the Secretary of Defense. The MA responsibilities of the commanders of ACOMs, ASCCs, and DRUs; USAR; and the CNGB include risk reduction for assets as well as ensuring that senior commanders understand the capability and status of all critical infrastructure on their installations, implement required risk mitigation strategies, and incorporate TCAs into their installation protection plans and emergency management plans.

(2) *Army proponent.* The DCS, G-3/5/7 is the Army's MA Lead (formerly Critical Infrastructure Assurance Officer).

(3) *Primary references.* DoDD 3020.40, and DoDI 3020.45, and AR 525-26.

j. Operations security.

(1) *General.* Commanders at all levels are responsible for ensuring that their units, activities, or installations plan, integrate, and implement OPSEC measures to protect their command's critical information in every phase of all operations, exercises, tests, or activities; and issuing orders, directives, and policies to protect their command's critical and sensitive information in order to clearly define the specific OPSEC measures that their personnel should practice.

(2) *Army proponent.* The DCS, G-3/5/7 is the proponent for OPSEC.

(3) *Primary reference.* AR 530-1.

(4) *Supporting reference.* DoDD 5205.02E and DoDM 5205.02.

k. Physical security.

(1) *General.* The Physical Security Program is the interrelationship of various components that complement each other to produce a comprehensive approach to security matters, including PS plans; PS inspections and surveys; participation in combating terrorism committees and fusion cells; and a continuing assessment of the installation's PS posture. The PS program encompasses the protection of certain assets: arms, ammunition, explosives, biological select agents and toxins, unclassified Army property, nuclear reactors and special nuclear materials, and chemical agents. The program accounts for the protection of Army sites, specifically controlling access to installations and stand-alone facilities and restricted area controls. The program also accounts for Army civilian police and security guards. The commanders of ACOMs, ASCCs, DRUs, the USAR, and CNGB PS responsibilities include establishing a PS program to plan and coordinate PS matters.

(2) *Army principal official.* The PMG assists in overseeing the Army PS Program.

(3) *Primary reference.* AR 190-13.

(4) *Supporting references.* ADP 3-37; AR 190-11; AR 190-17; AR 190-51; AR 190-54; AR 190-56; AR 190-59; ATP 3-39.32; DoD Directive-Type Memorandum 09-012; DoDI 5200.08; DoDI 5210.65; DoDM 5100.76; DoD Regulation 5200.08; Homeland Security Presidential Directive 12; and Title 50, United States Code, Section 797.

l. Security programs.

(1) *General.* The programs cover the management and execution of policies and procedures to ensure that acceptance and retention of personnel in the Armed Forces and United States Army, acceptance and retention of civilian employees in the DoD and DA, and granting members of the Armed Forces, Army, DA and DoD civilian employees, DA and DoD contractors, and other affiliated persons access to classified information and assignment to sensitive positions are properly executed as an integral part of the overall personnel Security Program. Program covers the comprehensive Security Program (SP) benchmarks: Intelligence Security Management, Personnel Security, Information Security, Industrial Security, Foreign Disclosure, SCI Management and Communications Security. DCS, G-2 assesses the command's security programs in determining proper execution at the Headquarters and Major Subordinate Command levels in meeting regulatory requirements. DCS, G-2 provides assistance to commanders of ACOMs, ASCCs, and/or DRUs in effectively managing their programs; identifying gaps in policy and devising solutions, plans of action, and recommendations for resourcing.

(2) *Army principal official.* The DCS, G-2 provides technical assistance and advice on the development and implementation of Army security programs.

(3) *Primary references.* DoDM 5200.02, AR 380-67, AR 380-5, AR 380-10, AR 380-28, AR 380-40, AR 380-49.

m. Suitability.

(1) *General.* The suitability program sets forth responsibilities concerning suitability, fitness, and credentialing for uniformed military personnel, civilians, volunteers, and contractors of the U.S. Army, as well as granting uniformed military personnel, civilians, contractors, volunteers, and other affiliated persons assignment to trusted positions. Suitability refers to a person's identifiable character traits or conduct that may have an impact on the integrity or efficiency of the service. Suitability is distinguishable from a person's ability to fulfill the qualifications of a job, as measured by experience, education, knowledge, and skills. Suitability and fitness have similar meanings; the distinction in usage relates to the populations of personnel under discussion. Suitability refers primarily to Federal civilian

and military employees. Suitability actions are actions taken that affect covered applicants and appointees under 5 CFR 731.203. Suitability actions consist of cancellation of eligibility for employment, removal, cancellation of reinstatement eligibility of employment or debarment after an unfavorable determination of suitability or fitness.

(2) *Army principal official.* The DCS, G-1 provides advice on the development of suitability, fitness, and credentialing functions.

(3) *Primary reference.* AR 600-78.

(4) *Supporting references.* Army Directive 2018-16, DoDI 1320.04, and 5 CFR 731.

B-2. Army Protection Program enabling functions

This section briefly identifies the APP enabling functions.

a. Intelligence and counterintelligence. Intelligence and counterintelligence (CI) activities support the APP by conducting collection, analysis, investigations, and operations designed to identify foreign intelligence and international terrorist activities that threaten the survivability and mission accomplishment of military personnel, civilian employees, contractors, and units. Army security helps protect classified and other protected information from loss, compromise, or unauthorized disclosure. Army intelligence and CI includes the areas of: all-source intelligence, counterintelligence, human intelligence, geospatial intelligence, imagery intelligence, measurement and signature intelligence, open-source intelligence, signals intelligence, and technical intelligence, information security, personnel security, industrial security, communications security, sensitive compartmented information, technical surveillance countermeasures, telecommunications electronics materiel protected from emanating spurious transmissions (TEMPEST), polygraph, foreign disclosure, special access programs, security education and training, and counterintelligence support to research and technology protection.

(1) *General.* Information sharing and/or fusion between Intelligence, CI, and CRIMINT. Fusion of CRIMINT, foreign intelligence and CI, with its resulting analytic product is fundamental to an effective security and force protection program and is required to support the APP. The APP safeguards DA resources through knowledge-based decision-making. In order to integrate, fuse, analyze and disseminate all-source threat information for commanders and force protection officials at all levels, all protection related activities must strive to integrate disparate threat-related data.

(2) *Army principal officials.*

(a) The DCS, G-2 coordinates on the development and oversight of policies and programs for Army intelligence and counterintelligence.

(b) The Director, USACID provide CRIMINT SME related to personnel security, criminal intelligence operations, suspicious activity reporting, computer crime intrusions, major procurement fraud, criminal activity in special access programs, and liaison for the exchange of critical threat and crime information with federal, state, tribal, and local LE agencies.

(3) *Primary references.* AR 381-10, AR 381-12, and AR 195-2.

(4) *Supporting references.* AR 380-5, AR 380-10, AR 380-27, AR 380-40, AR 380-49, AR 380-53, AR 380-67, AR 380-381, DoDD 5200.27, DoDD 5230.11, DoDD 5240.01, DoD Regulation 5240.1-R.

b. Security engineering.

(1) *General.* Security engineering services assist in protecting designated assets against criminal and terrorist threats, and military weapons effects. Security engineering services assist the commands and installations with structural damage surveys, vulnerability and protection assessments at fixed facilities and forward-deployed sites; consultation and preparation of facility drawings and specifications, on-site inspections and review of contract specifications and contractor submittals; revising protective design manuals and other publications, reports and regulations, and offering short courses that provide the tools to protect personnel and other critical assets against a wide range of threats. Security engineering also includes the design, construction, procurement and electronic security system project construction management for Intrusion Detection Systems and provides a wide range of electronic security system-related services.

(2) *Army principal official.* The USACE, through the commanders and district engineers, USACE Protective Design Centers, develops and maintains security engineering construction codes and provides security engineering services.

(3) *Primary references.* The Unified Facilities Criteria series of documents are available at <https://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc>.

Appendix C

Army Protection Program Governance Cycle at Headquarters, Department of the Army

C-1. Army Protection Program Board of Directors

a. General. The APPBOD—

(1) Serves as the principal forum responsible to recommend protection-related issues, requirements, and actions for decision to the appropriate Army senior leader.

(2) Operates as a senior-level collaborative forum promoting cross-functional, protection-related coordination and prioritization among HQDA APPBOD board members.

(3) Coordinates and integrates the APP primary functions and their associated enabling functions.

(4) Serves as a flexible mechanism to support the APP, comprehensively addressing non-warfighting protection policy issues, shaping program planning, supporting the PPBE process, ensuring effective integration with Army warfighting responsibilities, and ensuring a unified effort among all APP functions.

b. Specific outputs. Specific outputs include, but are not limited to the following:

(1) Recommending major APP transformation initiatives for input to TAP with associated tasks, milestones, and metrics.

(2) Recommending a balanced capabilities portfolio for the APP, reviewed on an annual basis.

(3) Reviewing and approving the protection priorities and APPL annually.

(4) Providing strategic guidance and assistance to APP program managers in preparing their programs.

(5) Specified Risk Management methodologies to include CJCSM 3105.01A and National Response Framework from the National Risk Management Center.

c. Frequency. Meets on a recurring basis as required, but no less than semi-annually, while ensuring timely incorporation of recommendations to the PPBE cycle.

d. Leadership. The ASA (M&RA) and DCS, G-3/5/7 co-chair the APPBOD.

e. Membership. The APPBOD is a principals-level body (three-star or equivalent). Membership may expand or contract, as appropriate with agenda topics, ensuring adequate issue coverage and comprised of representatives from the following:

(1) ASA (M&RA)—Co-chair.

(2) DCS, G-3/5/7—Co-chair.

(3) Under Secretary of the Army.

(4) ASA (FM&C).

(5) ASA (IE&E).

(6) ASA (ALT).

(7) General Counsel.

(8) Director of the Army Staff.

(9) AASA.

(10) CNGB.

(11) DCS, G-1.

(12) DCS, G-2.

(13) DCS, G-4.

(14) DCS, G-6.

(15) DCS, G-8.

(16) DCS, G-9.

(17) CIO.

(18) CAR.

(19) COE.

(20) TSG.

(21) TJAG.

(22) CCH.

(23) PMG.

f. Proxy and advisory capacity. When the above APPBOD board members are not available, they may designate a proxy to attend meetings for continuity purposes only. The chair and co-chair of the APPGOSC will serve on the APPBOD in an advisory capacity.

C-2. Army Protection Program General Officer Steering Committee

a. General. As a subcommittee to the APPBOD, the APPGOSC reviews, resolves, and assigns responsibility for APP topics, issues, and/or tasks appropriate to their level and assists the APPBOD in the development of key required outputs. The APPGOSC recommends courses of action for unresolved topics, issues, and/or tasks for APPBOD consideration and/or adjudication.

b. Frequency. Convenes as necessary, but not less than semi-annually.

c. Leadership. The DCS, G-3/5/7 (G-33), and the PMG co-chair the APPGOSC, with the ASA (M&RA) providing oversight. The DCS, G-3/5/7 (DAMO-ODP (G-34)) serves as a principal advisor to the co-chairs in addition to serving as the executive secretary.

d. Membership. The APPGOSC is comprised of one and two-star (or equivalent) general officers. Membership may expand or contract, as appropriate with agenda topics, ensuring adequate issue coverage. The APPGOSC is comprised of representatives from the following:

- (1) DCS, G-3/5/7 (G-33)–Co-chair.
- (2) PMG–Co-chair.
- (3) Under Secretary of the Army.
- (4) ASA (M&RA).
- (5) ASA (FM&C).
- (6) ASA (IE&E).
- (7) ASA (ALT).
- (8) General Counsel.
- (9) AASA.
- (10) CNGB.
- (11) Director of the Army Staff.
- (12) DCS, G-1.
- (13) DCS, G-2.
- (14) DCS, G-4.
- (15) DCS, G-6.
- (16) DCS, G-8.
- (17) DCS, G-9.
- (18) CIO.
- (19) CAR.
- (20) COE.
- (21) TSG.
- (22) TJAG.
- (23) CCH.

e. Army Protection Program General Officer Steering Committee membership. The APPGOSC membership may expand or contract, as appropriate with agenda topics, ensuring adequate issue coverage. The ACOMs and ASCCs are invited to participate in the APPGOSC with the appropriate level of representation. The DRUs are represented by their HQDA counterparts.

C-3. Army Protection Program Council of Colonels

a. General. The APPCOC is a subcommittee to the APPGOSC which reviews, resolves, and assigns responsibility for APP topics, issues, and/or tasks appropriate to their level and assists the APPGOSC in the development of key required outputs. For unresolved topics, issues, and/or tasks the APPCOC recommends courses of action for APPGOSC consideration and/or adjudication.

b. Frequency. Convenes as necessary, but not less than semi-annually.

c. Leadership. The APPCOC is co-chaired by a colonel (or equivalent) representative from both the DCS, G-3/5/7, DAMO – ODP (G – 34) and OPMG.

d. Membership. The APPCOC is comprised of colonel (or equivalent) representatives from the same organizations as listed in paragraph C-2 for the APPGOSC. Representatives from the APP primary functions and their associated enabling functions as listed in appendix B may participate in the APPCOC as desired. Membership may expand or contract, as appropriate with agenda topics, ensuring adequate issue coverage. The HQDA APP management forums may establish standing and/or temporary working groups as necessary. The ACOMs and ASCCs are invited to participate in the APPCOC with the appropriate level of representation. The DRUs are represented by their HQDA counterparts.

C-4. Army Protection Program Working Group

a. General. The APPWG is a subcommittee to the APPCOC which reviews, resolves, and assigns responsibility for APP topics, issues, and/or tasks appropriate to their level and assists the APPCOC in the development of key required outputs. The APPWG is co-chaired by a DAMO-ODP/G-34 Branch Chief and a representative from OPMG; it is the standard entry-level protection governance forum. The APPWG will implement business rules to establish controls for analyzing protection related issues and document and validate corrective actions. The APPWG will perform initial risk analysis of each protection-related issue to identify the desired outcome of the corrective action. Additionally, the APPWG will assign Offices of Primary Responsibility (OPRs) and Offices of Coordinating Responsibility, as well as identify minimum documentation requirements and approvals needed to present issues for validation and action to the APPCOC.

b. Frequency. Convenes as necessary, but not less than semi-annually.

c. Membership. The APPWG is comprised of representatives from the same organizations as listed in paragraph C – 2. Representatives from the APP primary functions and their associated enabling functions, as listed in appendix B, may participate in the APPWG as desired. Membership may expand or contract, as appropriate with agenda topics, ensuring adequate issue coverage for each protection issue. Commanders of ACOMs and ASCCs are invited to participate in the APPWG with the appropriate level of representation. Commanders of DRUs may participate or be represented by their HQDA counterparts.

d. The APPWG will establish and document a formal status monitoring process for ongoing protection-related issues, including a master listing with tentative completion dates and a periodic review of actions, to identify and resolve OPR challenges. The APPWG functions to approve issues for presentation at the APPCOC and prepare for each APPCOC, APPGOSC, and APPBOD. However, final decisions on protection issues, and closing unresolved actions is dependent upon the APPGOSC and APPBOD. In addition, the Army Protection Threat Working Group (APTWG) informs the APP governance process. The APTWG is designed to inform the HQDA staff and command of various threats that potentially drive requirements for force protection. This forum convenes quarterly to synchronize the threat picture.

e. In addition to meeting, any protection subcommittees may perform their functions through paper reviews.

f. The Chief, DAMO-ODP will maintain all supporting protection documentation for 3 years, as an effort to maintain a master listing of ongoing protection issues. Periodically, DAMO-ODP will conduct a review of open actions to identify and resolve OPR/OCR challenges to bring issues to closure.

Appendix D

Integrated Protection Plan Format for Commands, Agencies, Activities and Installations

See chapter 5 for applicable organizations and requirements.

D–1. Integrated protection plan

- a. Date of update. (Updated triennially.)
- b. General description of the command(s), sub-component(s), and their MEFs; identification of supporting commands, installation(s) and stand-alone facilities with associated figures, and general maps.
- c. Organization of the APP functions and their associated enabling functions within the command's operations-focused organization and how they are coordinated and synchronized. Description of the command(s)', sub-component(s)', installation(s)', and stand-alone facilities' capabilities of their protection primary functions and enabling functions.
- d. General descriptions of the most probable threats, hazards, and risks to the command and its supporting installation(s) and facilities. (Specific information at each supporting installation(s) and facility will be per para D–3.)
- e. Description, membership, responsibilities, and functions of the PEC and other protection-related forums, committees, councils, and working groups (such as EM, COOP, OPSEC, AT, Threat Working Group, PS Council, and so forth).
- f. Review of trend analysis (threats, hazards, incidents), strategic protection, and resiliency issues, the specific risks mitigated or accepted, and the date and name of accepting authority.
- g. Annual schedule of protection meetings, and training events. Address the consolidated and integrated full-scale protection exercise and identify the capabilities from all APP primary functions, and the command and control capabilities that will be exercised and the schedule for exercising all APP primary functions at least triennially (such as tabletop, functional, and/or full-scale).
- h. Approving signature of Commander or senior leader.

D–2. Mission essential functions, operational requirements, and critical assets

The organization's MEFs, other operational requirements, and critical assets identified and prioritized through mission analysis. (Classify appropriately.)

D–3. Identified and prioritized risks to mission essential functions, operational requirements, and critical assets

The identified and prioritized risks to the organization's MEFs, other operational requirements, and critical assets; based upon the most probable threats and hazards to the command and its supporting installation(s) and facilities. Threats, hazards, and risks may be identified by both integrated assessments and analysis. Prioritize risks and risk management efforts. (Classify appropriately.)

D–4. Directory of Army Protection Program functions and associated enabling functions

A directory of the organizational and supporting organizations' points of contact for the protection functions with points of contact for command(s)', sub-component(s)', installation(s)', and stand-alone facilities' protection functions and emergency operations center(s) phone numbers and email directories.

D–5. Established support agreements

MAAs, MOUs, MOAs, ISSAs, and support contracts available for coordinating response and recovery operations with civil and military partners; including coordination with local governments, first responders, NGOs, host nation, and the private sector (where applicable).

D–6. Command's protection plan guidance

A list of the commands, agencies, and/or activities' protection-related functional plans and operations orders of: (1) protection guidance from supported commands, and (2) protection guidance to subordinate commands. Includes a list of the IPPs of: supported commands; immediate subordinate commands (as applicable), supporting commands, agencies, and/or activities; and supporting installations and facilities' installation management plans.

D–7. Probable threats and hazards appendices

An appendix (as required) to address each command, agency, and/or activity-identified most probable threat and hazard with the efforts to prepare for, prevent against, respond to, and recover from the identified threat and hazard by

the integration of protection programs' activities. Use risk-informed decision-making to develop mitigation strategies. Reduce risk through cooperation and resource sharing. Identify resourcing activities through existing protection programs and future investments. Identify communications, command and control, and resources for response and recovery. Examples of threats and hazards could include: active shooters, hazardous material spills, cyberattacks and denial of services, utility disruptions, extreme weather events, pandemic events, events that requires relocation and activation of COOPs at each applicable installation and stand-alone facility.

Appendix E

Internal Control Evaluation

E-1. Function

The function covered by this evaluation is the APP.

E-2. Purpose

The purpose of this evaluation is to assist the Army Staff; commanders of ACOMs, ASCCs, and DRUs; the CNGB; the CAR; senior leaders of agencies and activities; senior commanders of installations; and the unit managers and internal control administrators in evaluating the key internal controls identified below in executing this regulation and implementing the APP. This evaluation is not intended to address all controls.

E-3. Instructions

Answers must be based on the actual testing of key internal controls (for example, document analysis, direct observation, sampling, and simulation). Answers that indicate deficiencies must be explained and corrective action indicated in supporting documentation. These controls must be formally evaluated at least once every 5 years. Certification that this evaluation has been conducted must be accomplished on DA Form 11 – 2 (Internal Control Evaluation Certification).

E-4. Test questions

a. Management and coordination.

- (1) Do the designated Army Staff sections and commands participate in the semi-annual APPBOD with the appropriate (three-star or equivalent) level of representation?
- (2) Do the designated Army Staff sections and commands participate in the semi-annual APPGOSC with the appropriate (one or two-star or equivalent) level of representation?
- (3) Do the designated Army Staff sections and commands participate in the semi-annual APPCOC with the appropriate (colonel or equivalent) level of representation?
- (4) Do the designated Army Staff sections and command participate in the semi-annual APPWG with the appropriate level of representation?
- (5) Have ACOMs, ASCCs, DRUs, USAR, CNGB, agencies, activities, and commanders established a PEC as the single, overarching protection forum to integrate and coordinate all APP primary functions and enabling functions?
- (6) Have ACOMs, ASCCs, DRUs, USAR, CNGB, agencies, activities, and commanders synchronized, integrated, and coordinated the APP primary functions and enabling functions and focused protection efforts on the command's, the Army's, and DoD's MEFs and operational requirements, within the operations section of the organization?
- (7) Are ACOMs, ASCCs, DRUs, USAR, CNGB, agencies, activities, and commanders of garrisons identifying and prioritizing MEFs and critical assets through a mission analysis and critical asset identification process?
- (8) Are ACOMs, ASCCs, DRUs, USAR, CNGB, agencies, activities, publishing an annual execution order for the fiscal year outlining the commands' APP priorities and integrated APP exercises for subordinate commands?
- (9) Are commands, agencies, and activities developing IPPs in accordance with appendix D?
- (10) Are IPPs of installations and stand-alone facilities written to support the requirements of the IPPs of their tenant commands, agencies, and activities?
- (11) Has the DCS, G-3/5/7 developed and disseminated to the ACOMs, ASCCs, and DRUs; USAR; CNGB; agencies and activities; and senior commanders an annual update of the APPL, identifying and rank-ordering installations utilizing an objective methodology that accounts for various factors, including standard garrison organization inputs, strategic functionality and criticality, and threat?

b. Assessments.

- (1) Are HQDA SMEs, from the APP primary functions, participating in triennial APPAs?
- (2) Are ACOMs, ASCCs, DRUs, USAR, CNGB, agencies and activities utilizing APP primary functions and the associated enabling functions SMEs to conduct tailored integrated higher headquarters protection assessments of their subordinate commands, a minimum of triennially?
- (3) Are ACOMs, ASCCs, DRUs, USAR, CNGB, agencies and activities within 90 days of the completion of a HQDA APP assessment, prioritizing and tracking identified vulnerabilities, developing a plan of action to mitigate or eliminate the vulnerabilities, and reporting all vulnerabilities documented by any assessment to DCS, G-3/5/7, DAMO-ODP (G-34)?

c. Exercises.

(1) Are Commanders at installations and standalone facilities planning and conducting a triennial consolidated and integrated protection exercise that includes capabilities from all primary protection functions, and evaluates APP command and control capabilities for the protection functions that are within their sphere of control and influence?

(2) Are Commanders at installations and stand-alone facilities ensuring all primary functions are exercised triennially, and conducting an exercise (such as tabletop, functional, and/or full scale) that evaluates the capabilities of all the APP primary functions?

E-5. Supersession

This evaluation replaces the previous evaluation, dated 8 December 2014.

E-6. Comments

Submit comments to make this checklist a better tool for evaluating internal controls to the DCS, G-3/5/7 (DAMO-OD), 400 Army Pentagon, Washington, DC 20310-0400.

Glossary

Section I

Abbreviations

ACOM

Army command

AOC

Army Operations Center

APP

Army Protection Program

APPA

Army Protection Program Assessment

APPBOD

Army Protection Program Board of Directors

APPCOC

Army Protection Program Council of Colonels

APPGOSC

Army Protection Program General Officer Steering Committee

APPL

Army Prioritized Protection List

APPWG

Army Protection Working Group

ARCYBER

U.S. Army Cyber Command

ARNG

Army National Guard

ASA (ALT)

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

ASA (FM&C)

Assistant Secretary of the Army (Financial Management and Comptroller)

ASA (IE&E)

Assistant Secretary of the Army (Installations, Energy and Environment)

ASA (M&RA)

Assistant Secretary of the Army (Manpower and Reserve Affairs)

ASCC

Army service component command

AT

Antiterrorism

AUAMP

Army User Activity Monitoring Program

CAR

Chief, Army Reserve

CG

commanding general

CI

counterintelligence

CIO
Chief Information Officer

CNGB
Chief, National Guard Bureau

COE
Chief of Engineers

COOP
Continuity of Operations

CRIMINT
Criminal Intelligence

CS
Cybersecurity

DA
Department of the Army

DAS
Director of the Army Staff

DCS
Deputy Chief of Staff

DoD
Department of Defense

DoDD
Department of Defense Directive

DoDI
Department of Defense Instruction

DRU
direct reporting unit

EM
emergency management

F&ES
Fire and Emergency Services

FHP
Force Health Protection

FM
Field Manual

FSE
full-scale exercise

HQDA
Headquarters, Department of the Army

IG
Inspector General

InT
insider threat

IPP
Integrated Protection Plan

ISSA
Inter-Service Support Agreement

JPEO

Joint Program Executive Office

JS

Joint Staff

LE

law enforcement

MA

mission assurance

MAA

Mutual Aid Agreement

MDEP

Management Decision Package

MEF

mission essential function

MOA

memorandum of agreement

MOU

memorandum of understanding

NGO

Non-Governmental Organization

OCR

Office of Coordinating Responsibility

OIP

Organizational Inspection Program

OPMG

Office of the Provost Marshal General

OPR

Office of Primary Responsibility

OPSEC

operations security

PEC

Protection Executive Committee

PEG

Program Evaluation Group

PEO

Program Executive Office

PMG

Provost Marshal General

POM

program objective memorandum

PPBC

Planning, Programming, Budgeting Committee

PPBE

Planning, Programming, Budgeting and Execution

PS

physical security

PTWG

Protection threat working group

PWG

Protection working group

RBE

reply by endorsement

SAP

Special Access Programs

SME

subject matter expert

TAP

The Army Plan

TCA

task critical asset

TEMPEST

Telecommunications Electronics Materiel Protected from Emanating Spurious Transmissions

THREAT

Threat Information Fusion & Reporting

TRADOC

U.S. Army Training and Doctrine Command

TSG

The Surgeon General

USACE

U.S. Army Corps of Engineers

USACID

U.S. Army Criminal Investigation Division

USAR

U.S. Army Reserve

USC

United States Code

Section II**Terms****Army Protection Program**

Formed to integrate, coordinate, synchronize, and prioritize protection policies and resources among the primary functions and the associated enabling functions.

Enabling Function

Army Program which supports a primary protection function.

Integrated Protection Plan

The integrating process for managing risks of the functions of protection to synchronize, integrate, and preserve the effectiveness and survivability of mission-related military and nonmilitary capabilities and assets—personnel, equipment, materiel, installations, facilities information and information systems, and infrastructure—in an all-threats and all-hazards environment.

Program Executive Office

The main stakeholder responsible for cost, schedule and performance in a DoD acquisition program and/or portfolio. A PEO may be responsible for a specific program (for example, the Joint Strike Fighter), or for an entire portfolio of similar programs.

Protection primary functions

An Army program that is a primary function of the APP, previously characterized as “pillars.”

Subordinate function

Army Program that is subordinate and contained within a primary function of the Protection program (for example, AT/INTEL). These programs are encapsulated within the primary function reflected as notations on the “pillars.”

UNCLASSIFIED

PIN 104677-000