Army Regulation 525–2

Military Operations

The Army Protection Program

Headquarters
Department of the Army
Washington, DC
8 December 2014

UNCLASSIFIED

SUMMARY

AR 525–2
The Army Protection Program

This new publication, dated 8 December 2014--

- Implements Army Directive 2011-04 (hereby superseded) and establishes the Army Protection Program to better manage risks relative to the safety and security of our Soldiers, civilians, family members, contractors, facilities, infrastructure, and information (para 1-1).

- Identifies Army Protection Program roles and responsibilities throughout the Army (chap 2).

- Identifies the Army Protection Program functional elements and associated enabling functions (para 3-1, app B).

- Outlines the implementation of the Army Protection Program (para 3-2).

- Uses a management framework that provides an enterprise approach to synchronize, integrate, prioritize, and coordinate protection programs, initiatives, and resources. The Headquarters, Department of the Army management structure provides Army Protection Program oversight, leadership, and governance by addressing protection-related issues (para 3-3).

- Outlines how the Army Protection Program will leverage existing management forums and the existing Army planning, programming, budgeting, and execution process (along with other management processes) to maintain relevant resource levels to address Army protection-related priorities and current and emerging threats and hazards (para 4-3).

- Defines the roles and responsibilities of the Protection Executive Committee as the executive management forum at commands, installations, and stand-alone facilities (para 5-1).

- Directs commands and agencies to identify and prioritize their mission essential functions and other operational requirements to identify and prioritize critical assets; and focus and prioritize protection efforts on their mission essential functions, other operational requirements, and critical assets (para 5-1*a*).

- Requires commands, agencies, activities, and subordinate commands as designated by their higher headquarters' commander and/or senior leader to develop integrated protection plans to address continued execution of designated mission essential functions, other operational requirements, and critical assets; and address preparation, prevention, protection, response, and recovery from all threats and hazards environments (para 5-1*b*).

- Encourages commands and installations to integrate and consolidate protection-related working groups of individual protection programs for efficiencies, while meeting the intent of individual protection-related program requirements and regulations (para 5-1*e*).

- Requires commands, installations, and stand-alone facilities to ensure their integrated protection plan and supporting functional plans support Headquarters, Department of the Army priorities, mission essential functions, and tenant and supported commands, agencies, and activities through all stages of events (para 5-1*f*).

- Implements Army Protection Program exercises and assessments to integrate and coordinate protection programs to assess capabilities and the ability to execute with external partners (paras 4-4, 5-3, and 5-4).

Headquarters
Department of the Army
Washington, DC
8 December 2014

*Army Regulation 525–2

Effective 8 January 2015

Military Operations

The Army Protection Program

By Order of the Secretary of the Army:

RAYMOND T. ODIERNO
General, United States Army
Chief of Staff

Official:

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

History. This publication is a new Department of the Army regulation.

Summary. This regulation implements Army Directive 2011–04 (hereby superseded) and establishes the Army Protection Program to better manage risks relative to the safety and security of our Soldiers, civilians, family members, facilities, contractors, infrastructure, and information. It prescribes policies, roles, responsibilities, and relationships across the Army Protection Program functional elements and their associated enabling functions to implement the Army Protection Program.

Applicability. This regulation applies to the Active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

Proponent and exception authority. The proponent agency 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 guidance.

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 lower echelon documents—such as plans, pamphlets, and similar supplements—with Deputy Chief of Staff, G–3/5/7 (G–34) coordination prior to publishing is authorized. Establishment of command and local forms is prohibited without prior approval from the Deputy Chief of Staff, G–3/5/7 (DAMO–OD), 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.

Committee management. AR 15-1 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, Department of the Army Committee Management Office (AARP-ZA), 9301 Chapek Road, Building 1458, Fort Belvoir, VA 22060-5527. Further, if it is determined that an established "group" identified within this regulation, later takes on the characteristics of a committee, as found in the AR 15-1, then the proponent will follow all AR 15-1 requirements for establishing and continuing the group as a committee.

Distribution. This publication is available in electronic media only and is intended for command levels C, D, and E for the Active 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 • 1–2, *page 1*
Explanation of abbreviations and terms • 1–3, *page 1*
Responsibilities • 1–4, *page 1*

*This regulation supersedes Army Directive 2011–04, dated 31 January 2011.

Contents—Continued

Statutory authority • 1–5, *page 1*
Civil liberties • 1–6, *page 1*
Precedence • 1–7, *page 1*

Chapter 2
Responsibilities, *page 1*
Assistant Secretary of the Army (Manpower and Reserve Affairs) • 2–1, *page 1*
Assistant Secretary of the Army (Financial Management and Comptroller) • 2–2, *page 1*
Assistant Secretary of the Army (Installations, Energy and Environment) • 2–3, *page 2*
Assistant Secretary of the Army (Acquisition, Logistics and Technology) • 2–4, *page 2*
Chief Information Officer, G–6 • 2–5, *page 2*
The General Counsel • 2–6, *page 2*
The Inspector General • 2–7, *page 2*
The Administrative Assistant to the Secretary of the Army • 2–8, *page 2*
Director of the Army Staff • 2–9, *page 2*
Deputy Chief of Staff, G–3/5/7 • 2–10, *page 2*
Deputy Chief of Staff, G–2 • 2–11, *page 4*
Deputy Chief of Staff, G–8 • 2–12, *page 4*
Deputy Chief of Staff, G–1 • 2–13, *page 4*
Deputy Chief of Staff, G–4 • 2–14, *page 4*
The Assistant Chief of Staff for Installation Management • 2–15, *page 4*
The Provost Marshal General • 2–16, *page 4*
Chief of Engineers • 2–17, *page 5*
The Surgeon General • 2–18, *page 5*
Chief, U.S. Army Reserve • 2–19, *page 5*
Chief, Army National Guard Bureau • 2–20, *page 5*
The Judge Advocate General • 2–21, *page 5*
Chief of Chaplains • 2–22, *page 5*
Commanders of Army commands, Army service component commands, and direct reporting units • 2–23, *page 5*
Commanding General, U.S. Training and Doctrine Command • 2–24, *page 5*
Commanding General, U.S. Army Cyber Command • 2–25, *page 5*
Commanding General, U.S. Army Corps of Engineers • 2–26, *page 5*
Commanding General, U.S. Army Criminal Investigation Command • 2–27, *page 6*
State Adjutants General • 2–28, *page 6*

Chapter 3
The Army Protection Program, *page 6*
Army Protection Program functional elements and enabling functions • 3–1, *page 6*
The Army Protection Program implementation • 3–2, *page 7*
Army Protection Program management structure • 3–3, *page 8*

Chapter 4
Headquarters, Department of the Army, *page 8*
Army Protection Program activities at Headquarters, Department of the Army • 4–1, *page 8*
Army Protection Program management structure at Headquarters, Department of the Army • 4–2, *page 9*
Planning, programming, budgeting, and execution cycle • 4–3, *page 9*
Army Protection Program assessments • 4–4, *page 10*

Chapter 5
Commands, agencies, activities, and installations, *page 10*
Planning and integration • 5–1, *page 10*
Training • 5–2, *page 12*
Exercise integration • 5–3, *page 12*
Assessing • 5–4, *page 12*
Evaluating • 5–5, *page 13*

Contents—Continued

Appendixes

A. References, *page 14*

B. The Army Protection Program Functional Elements and Enabling Functions, *page 21*

C. Army Protection Program Management Structure at Headquarters, Department of the Army, *page 25*

D. Base Integrated Protection Plan Format for Commands, Agencies, and Activities., *page 27*

E. Internal Control Evaluation, *page 28*

Figure List

Figure 3–1: Army Protection Program's functional elements and enabling functions, *page 6*

Glossary

Chapter 1
Introduction

1–1. Purpose
This regulation establishes the Army Protection Program (APP) to better manage risks relative to the safety and security of our Soldiers, civilians, family members, contractors, facilities, infrastructure, and information. The APP is the overarching management program for synchronizing, integrating, coordinating, and prioritizing policies, decisions, and resources of the 12 non-warfighting APP functional elements and the three APP enabling functions as identified in paragraph 3–1. This regulation prescribes policies, roles, responsibilities, and relationships across the APP functional elements and their associated enabling 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 decisionmaking and resource allocation in an all threats and hazards environment.

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

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

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

1–5. Statutory authority
Statutory authority for this regulation is derived from Section 3013, Title 10, United States Code.

1–6. Civil liberties
This regulation addresses activities where information is obtained, shared, and used in the interest of protecting persons, property, and other elements of national security. Through the APP the Army's leadership provides oversight to ensure civil liberties are not encroached upon while collecting information. The APP follows U.S. laws and Department of Defense (DOD) and Army policies to protect civil liberties and ensure freedoms are not infringed upon. The intent of the APP is to comply with civil liberties requirements while accomplishing the Army's mission of protecting the Nation and the constitutional freedoms of its citizens.

1–7. Precedence
This regulation is the proponent policy document for the APP. All other policies, including but not limited to, regulations, pamphlets, and/or other documents of the APP functional elements will comply with this regulation within 18 months from date of publication. If at any time there is a conflict in this regulation with any other APP-related Army policy, including other Army regulations, this regulation takes precedence.

Chapter 2
Responsibilities
The responsibilities listed in this regulation are specifically in support of the APP and are supplemental to any other responsibilities in applicable directives, policies, regulations, or laws. In addition to the responsibilities listed below, all Headquarters, Department of the Army (HQDA) principal officials, commanders, Army organizations, and personnel will support the DCS, G–3/5/7 in executing this regulation and implementing the APP.

2–1. Assistant Secretary of the Army (Manpower and Reserve Affairs)
The ASA (M&RA) will—

a. Serve as the Army Secretariat lead for oversight of the APP and ensure the close coordination of oversight efforts across the Secretariat, particularly with the Assistant Secretary of the Army (Financial Management and Comptroller) (ASA (FM&C)) and the Assistant Secretary of the Army (Installations, Energy and Environment) (ASA IE&E) to ensure that fiscal and installation concerns are properly addressed.

b. Serve as a co-chair of the APP Board of Directors (APPBOD) and provide representation to the APP General Officer Steering Committee (APPGOSC) and APP Council of Colonels (APPCOC).

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

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

2–2. 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 and APPCOC.

b. Assist the DCS, G–3/5/7 (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 subject matter experts (SMEs) to assist the DCS, G–3/5/7 (G–34) in synchronizing protection-related issues influencing multiple MDEPs and program evaluation groups (PEGs) to reduce redundant efforts across the APP.

2–3. 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 and APPCOC.

b. Assist the DCS, G–3/5/7 (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.

2–4. 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 APPGOSC and APPCOC.

b. Provide 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.

2–5. Chief Information Officer, G–6

The CIO/G–6 will—

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

b. Serve as the APP lead for the information assurance (IA) functional element of protection and its associated enabling functions.

2–6. The General Counsel

The General Counsel will serve as a member of the APPBOD and provide representation to the APPGOSC and APPCOC.

2–7. The Inspector General

The IG will provide on request redacted inspection-report findings related directly to the APP and any unattributed assistance or investigatory trends that may help identify critical APP gaps, and for inclusion in external APP reports.

2–8. The Administrative Assistant to the Secretary of the Army

The Administrative Assistant to the Secretary will—

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

b. Implement the APP for HQDA, its field operating agencies, staff support agencies, and specified direct reporting units (DRUs) per DA General Order 2012–01 and Army Regulation (AR) 10–87 by performing the responsibilities listed in chapter 5 of this regulation.

c. Develop the protection program necessary in HQDA agencies to ensure effective protection and awareness across the HQDA staff and Secretariat agencies.

2–9. Director of the Army Staff

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

2–10. 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 principal officials 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 principal officials and commanders carry out their protection-related duties in a coordinated and integrated fashion.

c. Serve as a co-chair of the APPBOD. Designate the DCS, G–3/5/7 co-chair for both the APPGOSC and APPCOC.

d. Support the HQDA APP management framework by providing the 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 for 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, taskings, 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 15–1.

(8) Ensure the work for the APPBOD is coordinated with other relevant Army enterprise-level bodies, Office of the Secretary of Defense (OSD), other Services, and Federal agencies, where appropriate.

e. Ensure the APP strategy and policy is appropriately linked with and nested under the DOD and JS protection-related programs.

f. Synchronize the exchange of protection information with the DOD, JS, and other Services to adopt best practices and improve protection policies and processes.

g. Develop and maintain a strategic plan for Army protection that synchronizes all the protection functional elements. Periodically review and adjust to evolving concepts, structure, and threats. Integrate appropriate protection priorities and strategy into periodic strategic documents, including, but not limited to The Army Plan (TAP).

h. Develop an annual Army Protection Posture Statement through the consolidation of information reported through the installation status report (ISR), unit status report (USR), assessment reports, and other sources and submit the Army Protection Posture Statement through the HQDA APP management structure for review and approval.

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. Oversee appropriate protection-related training.

k. Conduct activities to ensure an integrated protection program is developed as part of the planning, programming, budgeting, and execution (PPBE) process by—

(1) Ensuring cross-MDEP and PEG integration and synchronization consistent with the APP programming guidance priorities.

(2) Evaluating competing requirements and preparing recommendations for consistency with APP priorities.

(3) Conducting an assessment of proposed Program Objective Memorandum (POM) funding levels to ensure the APP strategy and supporting programs are defendable and executable.

l. Ensure DA level protection priorities and requirements are disseminated to the Army commands (ACOMs), Army service component commands (ASCCs), DRUs, United States Army Reserve (USAR), and the Army National Guard (ARNG).

m. Coordinate Army non-warfighting protection enabling functions as listed in appendix B.

n. 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 flows and information sharing capabilities by—

(1) Maintaining an APP portal site 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) Review protection-related responses (for example, Congressional testimony, Government Accountability Office requests, and IG inspections) to highlight issues to refer to the APPBOD.

(3) Publishing the Army Planning Priorities Guidance and APPL annually to senior commanders communicating strategic missions, assets, and capabilities.

(4) Coordinating with the Assistant Chief of Staff for Installation Management (ACSIM) 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.

(5) 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.

(6) Ensuring HQDA APP management framework priorities and recommendations are reflected in protection-related DA directives, regulations, pamphlets, orders, and messages.

o. Coordinate Army Protection Program Assessments (APPAs). Maintain a list of APPA benchmarks and make them available to the commands by a portal.

p. Serve as the APP lead for the continuity of operations, emergency management (EM), critical infrastructure risk management, and operations security (OPSEC) functional elements of protection.

2–11. 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 and APPCOC.

b. Serve as the APP lead for foreign intelligence; international terrorism; counterintelligence; personnel, industrial, and information security; and foreign disclosure and sensitive compartmented information management as they relate to or enable the APP.

c. Synchronize Security Resiliency program initiatives with the Army Insider Threat Program.

d. Develop and continuously maintain security measures to address gaps in the areas of personnel security and counterintelligence.

e. Recommend protection-related information and collection requirements to Army leaders in support of the APP.

f. In coordination with the CIO/G–6, serve as the APP lead for IA of Army Intelligence Community Networks.

g. Facilitate Information Sharing between the counterintelligence and law enforcement (LE) activities in order to provide commanders early warning of potential and emerging threats.

2–12. 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 and APPCOC.

b. Provide SMEs 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 PPBE actions and POM development.

c. In coordination with DCS, G–3/5/7 (G–34), maintain a list of direct and indirect APP MDEPs and update the list annually.

2–13. Deputy Chief of Staff, G–1

The DCS, G–1 will serve as a member of the APP BOD and provide representation to the APPGOSC and APPCOC.

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 and APPCOC.

2–15. The Assistant Chief of Staff for Installation Management

The ACSIM will—

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

b. Serve as the APP lead for the fire and emergency services (F&ES) functional element of protection.

c. Ensure the Installations Program Evaluation Group (II PEG) adequately addresses protection-related priorities throughout the PPBE process.

d. In coordination with DCS, G–3/5/7 (G–34), incorporate the APP into the ISR and provide ISR data to support DCS, G–3/5/7 (G–34) in developing an annual Armywide protection report that consolidates ISR feedback from commands and installations.

e. Provide access to manpower models and other protection-related data to the DCS, G–3/5/7 (G–34) from the Standard Garrison Organization Model and other databases that supports or impacts protection-related services.

f. In coordination with DCS, G–3/5/7 (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.

g. Assist the DCS, G–3/5/7 in planning, programming, and executing protection-related activities at Army installations and separate facilities.

2–16. The Provost Marshal General

The PMG will—

a. Serve as a member of the APPBOD.

b. Serve as a co-chair of APPGOSC.

c. Designate an O–6 level (or equivalent) representative to co-chair the APPCOC.

d. Designate a liaison to the DCS, G–3/5/7 (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 (CAT), OPMG will provide a liaison to support the DCS, G–3/5/7 (G–34).

e. Serve as the APP lead for the high-risk personnel (HRP), LE, physical security (PS), and antiterrorism (AT) functional elements of protection and their associated enabling functions.

f. 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 Branch and Army Threat Integration Center (ARTIC) functions and supporting the ASA (IE&E) on installation PS.

g. Provide recommendations to the DCS, G–3/5/7 for inclusion in annual protection priorities.

2–17. Chief of Engineers

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

2–18. The Surgeon General

TSG will—

a. Serve as a member of the APPBOD and provide representatives to the APPCOC and APPGOSC.

b. Serve as the APP lead for the health protection (HP) functional element of protection and its associated enabling functions.

c. Ensure protection considerations are integrated into HP contracting.

2–19. Chief, U.S. Army Reserve

The CAR will—

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

b. Publish guidance to subordinate commands concerning implementation of the APP, including establishing Protection Executive Committee (PEC), developing integrated protection plans, and conducting consolidated and integrated protection exercises.

2–20. Chief, Army National Guard Bureau

The CNGB will—

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

b. Publish guidance to all State adjutants general concerning implementation of the APP, including establishing PECs, developing integrated protection plans, and conducting consolidated and integrated protection exercises.

c. Ensure the Director, ARNG executes the APP per chapter 5.

2–21. The Judge Advocate General

The Judge Advocate General will serve as a member of the APPBOD and provide representation to the APPGOSC and the APPCOC.

2–22. Chief of Chaplains

The Chief of Chaplains will serve as a member of the APPBOD and provide representation to the APPGOSC and APPCOC.

2–23. 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.

2–24. Commanding General, U.S. Training and Doctrine Command

The CG, TRADOC will—

a. Determine capability gaps and identify solutions to support the APP.

b. Submit APP-related doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) requirements to the HQDA APP forums for validation.

2–25. Commanding General, U.S. Army Cyber Command

The CG, ARCYBER will serve as the APP lead for the Computer Network Defense (CND) functional element of protection and its associated enabling functions.

2–26. 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. Ensure, as the defense critical infrastructure program lead agency for Defense Public Works Sector, the coordination of Defense Sector Public Works outputs that impact the APP with the DCS, G–3/5/7.

c. Leverage USACE Centers for Excellence for best practices to support the APP enabling functions and make geographic information systems (GIS) data available to support protection-related activities.

d. Integrate protection considerations into public works projects as appropriate.

2–27. Commanding General, U.S. Army Criminal Investigation Command

To the extent permitted by applicable law and regulation, the CG, USACIDC will provide criminal intelligence (CRIMINT) to identify domestic terrorist and extremist activities, and criminal activities such as insider threats in support of the APP's Intelligence fusion enabling function described in appendix B.

2–28. State Adjutants General

State Adjutants General, based upon DARNG guidance, will publish guidance for all subordinate commands concerning implementation of the APP, to include state specific guidance concerning the implementation of—

a. PECs and working groups.

b. Developing EM and integrated protection plans.

c. Conducting consolidated and integrated protection training and exercises.

Chapter 3
The Army Protection Program

3–1. Army Protection Program functional elements and enabling functions

a. The APP enables the execution of Army missions in all threats and hazards environments and by integrating, coordinating, synchronizing, and effectively prioritizing the efforts and resources of the APP functional elements and enabling functions, with their associated risk management processes. The APP supports operational objectives and serves as the primary means for the Army to support the execution of the DOD Mission Assurance Strategy. Figure 3–1 shows the APP's non-warfighting functional elements arranged vertically and the enabling functions arranged horizontally across the bottom of the figure.

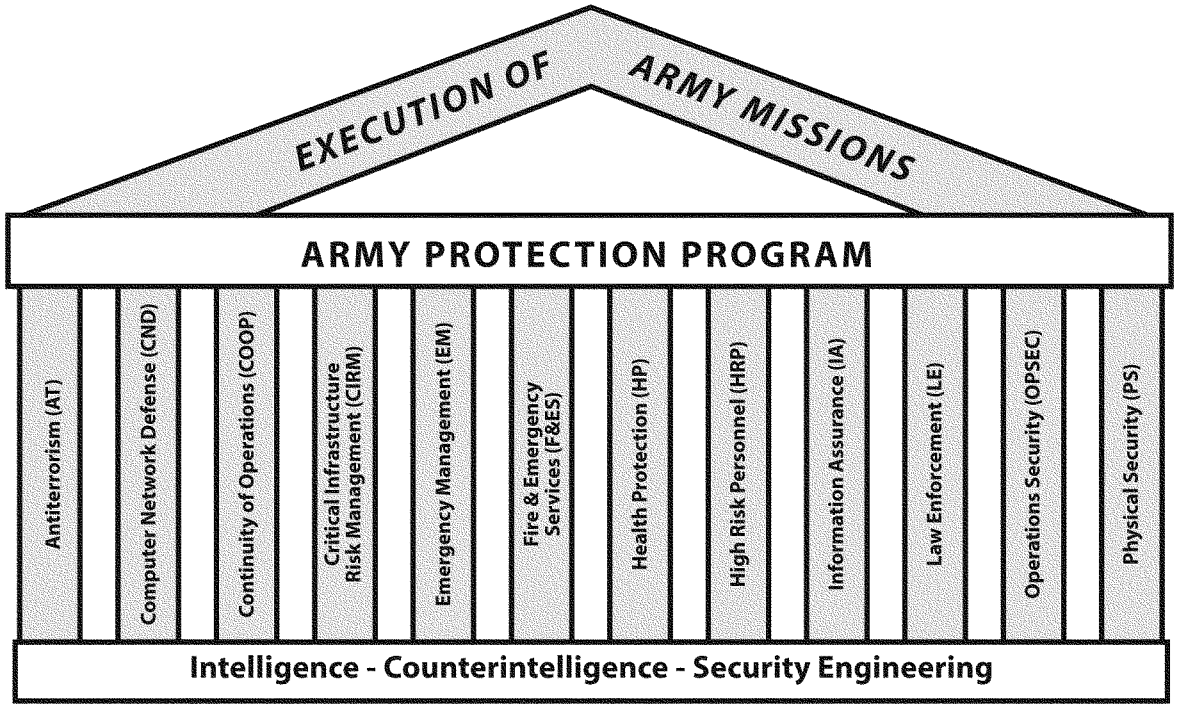

Figure 3–1. Army Protection Program's functional elements and enabling functions

b. The APP is comprised of the following non-warfighting functional elements and associated enabling functions:

(1) *Functional elements*. The functional elements of the APP are: AT, CND, Continuity of Operations, Critical Infrastructure Risk Management, EM, F&ES, HP, HRP, IA, LE, OPSEC, and PS. Additional information about the APP's functional elements can be found in section I of appendix B.

(2) *Enabling functions*. The enabling functions of the APP are: Intelligence, Counterintelligence, and Security Engineering Services. Additional information about the APP's enabling functions can be found in section II of appendix B.

3–2. The Army Protection Program implementation

The APP unifies the protection effort to support the execution of Army missions and DOD mission essential functions (MEFs) in an all threats and hazards environment by integrating, coordinating, synchronizing, and effectively prioritizing the efforts and resources of the APP functional elements and enabling functions. The APP does not seek to eliminate the risks of threats and hazards, but seeks to prevent, prepare, protect, mitigate, respond, and recover from an event to minimize the impact on the execution of DOD and Army missions.

a. Commanders at all levels will consider the following when managing the risk to DOD's and the Army's MEFs and other operational requirements:

(1) *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.

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

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

(c) 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.

(2) *Risk-informed culture*: A risk-informed culture supports protection activities. It relies on vigilance and situational awareness to support information sharing and risk-informed decisionmaking. Leaders are aware of the full spectrum of threats and prepare plans to effectively continue operational requirements.

(a) 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 our 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.

(b) Information sharing and risk-informed decisionmaking. Appropriate, accessible, and timely information allows for the ongoing analysis of risks and assessment of best practices. Risk-informed decisionmaking 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.

(3) *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.

(a) 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.

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

(c) 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.

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

(a) 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.

(b) Accountability. The APP expands program oversight, promotes leader accountability, and better facilitates informed decisionmaking and resource allocation.

(5) *End-state focus*: The APP provides leaders and decision makers in each of the functional elements with actionable information based on consistent assessments and analyses.

(a) Actionable information. Assessments and analyses directly support mission-focused integrated protection decisionmaking and inform the PPBE process.

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

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

(6) *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.

b. 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) Proactively linking strategic risk management decisions to support operational requirements and critical functionality.

(2) Coordinating across protection stovepipes and creating a more complete and accurate understanding of risks.

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

(4) Integrating multiple risk management programs and assessment methodologies.

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

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

3–3. Army Protection Program management structure

The APP management structure 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 management structure consists of APPBOD, APPGOSC, APPCOC, and associated working groups, as required. At the HQDA level, the APP expands program oversight, ensures senior leader accountability, and facilitates informed decisionmaking and resource allocation (see para 4–2).

b. The PEC is the APP management structure 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 functional elements of protection (see para 5–1).

Chapter 4
Headquarters, Department of the Army

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

The HQDA APP principal officials develop, integrate, and synchronize protection policies, plans, programs, and resource investments to proactively link strategic risk management decisions to operational requirements and critical functionality. HQDA APP principal officials coordinate Army priorities in concert with the geographic combatant commander's theater priorities.

a. HQDA APP principal officials will—

(1) Evaluate Armywide risk by reviewing trends analysis, discussing strategic protection and resiliency issues, and advocating acceptance, mitigation, or resolution of risk.

(2) Develop and annually update the APP Posture Statement.

(3) Develop and annually update the Army strategic protection priorities.

(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) Provide input to TAP and other strategic guidance.

(6) Inform senior leaders.

(7) Prioritize risk management efforts to increase programming and budgeting efficiencies, eliminate unnecessary

redundancies, achieve closer integration of key activities, and better inform the resourcing of existing programs and future investments.

b. The HQDA APP principal officials reduce risk through shared responsibility.

(1) The HQDA APP management structure is the issue-based collaborative structure that implements and oversees the Armywide integrated protection process.

(2) 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 (JPEO) (for example, JPEO Chemical, Biological 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.

c. The HQDA principal officials identified in chapter 2 who manage and execute the functional elements 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) Ensure all existing policies, including but not limited to, regulations, pamphlets, and/or other documents comply with this regulation within 18 months from date of publication.

(3) Coordinate and synchronize all primary regulations related to the APP non-warfighting functions, as outlined in appendix B prior to revision or publication.

(4) Coordinate key protection-related decisions, issues, policies, and concerns with the HQDA APP management structure prior to implementation, publication, or execution.

(5) Identify program priorities, emerging issues, and other protection-related topics for inclusion in TAP and other strategic documents through the HQDA APP management structure.

(6) Coordinate all fielding or implementation sequencing of protection actions at installations and facilities with the DCS, G–3/5/7 (G–34).

4–2. Army Protection Program management structure at Headquarters, Department of the Army

HQDA is responsible for providing oversight, leadership, and governance for the overall APP. The HQDA APP management structure is comprised of three forums: the APPBOD, APPGOSC, and APPCOC; whose composition and responsibilities are defined in appendix C**.**

4–3. Planning, programming, budgeting, and execution cycle

This regulation does not change current functional proponency for MDEPS. The APPBOD's executive secretary within the DCS, G–3/5/7 (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 management structure 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. 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 management structure, the APP develops overarching strategic guidance for inclusion in TAP, as well as, tailored programmatic guidance for program and/or MDEP managers to align APP priorities with DOD and Army senior leader priorities. The DCS, G–3/5/7 will—

(1) Ensure the APP strategy is incorporated into the development of the Army Strategic Planning Guidance and the Army Campaign Plan.

(2) Ensure APP requirements are considered during the development of the Army Planning Priorities Guidance.

(3) Ensure the APP requirements are considered during the development of the Army Program Guidance Memo.

(4) Ensure APP requirements are validated, prioritized, analyzed, and integrated for protection-related capability integration requirements.

(5) Ensure APP requirements are addressed at PPBC meetings involving protection-related issues.

(6) Ensure coordination with the APP functional elements and associated enabling functions.

(7) Ensure the full spectrum of Army assets are addressed, to include installations and stand-alone facilities

b. Programming. Through the HQDA APP management framework, the DCS, G–3/5/7 develops annual protection-related requirements guidance and facilitates cross-MDEP and/or -PEG synchronization and coordination to ensure APP equities are adequately addressed in the POM process.

(1) HQDA APP management framework develops overarching protection-related programming guidance based on TAP and other senior leader priorities.

(2) In coordination with DCS, G–3/5/7 (G–34), DCS, G–8 (Program Analysis and Evaluation) will develop a list of direct APP focused MDEPs.

(3) MDEP managers of direct APP MDEPs will—

(a) Develop individual program guidance in accordance with APPBOD guidance and priorities.

(b) Provide MDEP requirements to the HQDA APP executive secretary prior to submission to the PEG.

(4) The DCS, G–3/5/7 will—

(a) Attend PPBC meetings involving protection-related issues.

(b) Participate in MDEP brief to respective PEG for each direct MDEP and indirect MDEPs, as needed.

(5) The APPBOD publishes a POM summary to capture final POM position and prioritization.

c. Budgeting. In coordination with the HQDA APP management framework, DCS, G–3/5/7 will—

(1) Attend PPBC meetings involving protection-related issues.

(2) Coordinate with ASA (FM&C) budget integration and formulation, impacted commands and programs during the resource management decision (RMD) cycle for protection-related draft RMDs.

(3) 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 (G–34) will—

(1) Attend PPBC meetings involving protection-related issues.

(2) Coordinate with ASA (FM&C) semi-annually to monitor protection-related execution data to maintain visibility of expenditures at the command, MDEP, and Army Program Element levels.

(3) Prepare execution summary report to the HQDA APP management framework on protection-related expenditures.

4–4. Army Protection Program assessments

a. DCS, G–3/5/7 (G–34), in coordination with HQDA SMEs from the APP functional elements and their associated enabling functions, will conduct triennial assessments of ACOMs, ASCCs, DRUs, and 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). The G–34 will normally participate in each APPA, mission requirements permitting.

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

c. DCS, G–3/5/7 (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) Publish an annual message identifying and disseminating trends Armywide, including best practices and awards.

(4) Approve special assessment areas for APPAs.

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

(6) Chair a semi-annual observation resolution board to track corrective actions from APPAs and associated Reply By Endorsements (RBEs).

Chapter 5
Commands, agencies, activities, and installations

The APP facilitates commands, installations, and stand-alone 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 the CAR; 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 CAR; 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 with applicable geographic combatant command (GCC) theater policies 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 integrated protection plans (IPPs) as per appendix D, exercise requirements and priorities, or be included in the commands' PEC and IPP.

c. Ensure protection-related programs are assessed as part of the command's Organizational Inspection Program and protection assessments complement rather than duplicate each other.

d. Within the command's operations (G–34 or similar) organization, synchronize, integrate, and coordinate the APP functional elements 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 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 supporting and enabling program 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, 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) Ensure subordinate commands' and organizations' protection requirements are coordinated with supporting commands, down to the installation(s) and/or separate facility where they reside.

(3) 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.

(4) 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; and 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 annually, and approved by the commander or senior leader.

(5) 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.

(6) 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).

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

(8) 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 functional elements to ensure mission accomplishment.

(9) Inform the Army Operations Center 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.

g. Senior commanders, leaders, and staff 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. Senior commanders and leaders at installations and/or stand-alone facilities, in addition to the above, will—

(1) Chair the installation and/or separate facility PEC with membership including the garrison commander, staff principals representing the APP functional elements, tenant commands, and other representatives as designated by the chair.

(2) Consider tenant organizations' requirements and include them in protection-related working groups.

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

(4) Integrate and leverage resource investments across the APP functional elements.

(5) Promote information sharing and unity of effort among APP functional elements and tenant organizations.

(6) Ensure all organic (such as engineer, medical, LE, PS) and tenant protection plans are incorporated into the overall installation protection plans.

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

(8) Develop protection-related guidance and standards to address the vetting and security of non-U.S. citizens and high-risk individuals; such as contract linguists, contract role players, and military accessions vital to national interest (MAVNI) personnel who access Army installations and facilities. Coordinate with the DCS, G–2 for the most current guidance and procedures regarding contract linguists, contract role players, and MAVNI personnel.

(9) 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).

(10) Ensure appropriate protection-related measures are incorporated into the contract process and vendor activities.

(11) Ensure IPPs and supporting functional plans support HQDA priorities, MEFs and tenant and supported commands, agencies, and activities through all stages of events.

5–2. Training

APP functional element protection-related training guidance will be integrated into commanders' annual training guidance to subordinate and tenant commands. Units 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 meet the individual APP functional elements' exercise requirements by planning, conducting, and participating in integrated protection exercises that include:

(1) Annually: At least one full-scale integrated protection exercise that includes capabilities from multiple APP functional elements, evaluates command and control capabilities for the protection elements, and is externally evaluated at least every other year. Those APP functional elements not included in the annual full-scale integrated exercise will be exercised during the year to meet APP functional elements' exercise requirements using seminars, tabletops, or functional exercises that integrate multiple APP functional elements and command and control capabilities.

(2) At least triennially: The capabilities of all the APP functional elements and command and control capabilities must be included in a full-scale protection exercise that is within the command's sphere of control and influence.

b. Include external partners for appropriate participation in integrated protection exercises per existing MAAs, MOUs, MOAs, and ISSAs for both response and consequence management phases.

c. Senior 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 functional capabilities must be captured in an after-action report and corrective actions implemented in order to receive exercise credit.

d. Provide an after-action report at the applicable classification level of each full-scale protection exercise with lessons learned to the higher headquarters and courtesy copy the DCS, G–3/5/7 (G–34) within 90 days of the exercise. After-action reports of full-scale protection exercises will be maintained for a minimum of three (3) years.

5–4. Assessing

Commands will ensure protection related programs are assessed as part of their Organizational Inspection Program and assess subordinate commands to ensure proper execution and overall compliance with the APP-related protection programs; and evaluate the command's training and exercise programs, the risk management decision processes, and identify trends and best practices.

a. Utilize SMEs from the APP functional elements and the associated enabling functions to conduct tailored and integrated assessments of their subordinate commands, a minimum of triennially, using the assessment benchmarks maintained by the HQDA G–34 at the designated portal. Integrate the assessment of specific protection programs requirements as prescribed by the applicable regulatory guidance.

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, Army Safety Office) whenever possible. When appropriate, Commands may

use external assessments to meet higher headquarters' assessment requirements. ACOMS, ASCCs, and DRUs will inform the DCS, G–3/5/7 (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 functional element(s), 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. Report all discrepancies and/or vulnerabilities documented by any assessment via the applicable APP functional element's DOD system of record (such as the Mission Assurance Risk Management Systems (MARMS)).

d. ACOMS, ASCCs, and DRUs will forward an annual trend analysis of subordinate commands' assessment results to the DCS, G–3/5/7 (G–34) by 30 June to conduct programmatic analysis and facilitate the efficient and effective PPBE of protection-related resources to meet identified Army requirements.

5–5. Evaluating

a. Commanders and senior leaders will evaluate all APP functional elements every year 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 policy and DOTMLPF solutions to improve protection risk management and build resiliency at the command or installation level. Forward recommended APP best practices and DOTMLPF changes to the DCS, G–3/5/7 (G–34).

c. Staff assistance visits for select APP areas can be requested from HQDA through the DCS, G–3/5/7 (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 Web site at http://www.apd.army.mil; DOD publications are available at http://www.dtic.mil/whs/directives/; Chairman of the Joint Chiefs of Staff publications are available at http://www.dtic.mil/doctrine/; and Unified Facilities Criteria (UFC) publications are available at http://www.wbdg.org/ccb/browse_cat.php?c=4.

AD 2013–18
Army Insider Threat Program

ADP 3–37
Protection

ADRP 3–37
Protection

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 15–1
Committee Management

AR 25–1
Army Information Technology

AR 25–2
Information Assurance

AR 25–30
The Army Publishing Program

AR 40–5
Preventive Medicine

AR 40–501
Standards of Medical Fitness

AR 40–562
Immunizations and Chemoprophylaxis for the Prevention of Infectious Disease

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 Dogs

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 Property (Sensitive and Nonsensitive)

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
Personal Security

AR 190–59
Chemical Agent Security Program

AR 195–2
Criminal Investigation Activities

AR 195–5
Evidence Procedures

AR 380–5
Department of the Army Information Security Program

AR 380–10
Foreign Disclosure and Contacts with Foreign Representatives

AR 380–27
Control of Compromising Emanations

AR 380–40
Safeguarding and Controlling Communications Security Materiel

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 (SAs)

AR 381–10
U.S. Army Intelligence Activities

AR 381–12
Threat Awareness and Reporting Program

AR 381–20
The Army Counterintelligence Program

AR 420–1
Army Facilities Management

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

AR 525–13
Antiterrorism

AR 525–26
Infrastructure Risk Management (Army)

AR 525–27
Army Emergency Management Program

AR 530–1
Operations Security (OPSEC)

AR 600–20
Army Command Policy

AR 600–63
Army Health Promotion

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

ATTP 3–39.20
Police Intelligence Operations

ATTP 3–39.32
Physical Security

Chairman of the Joint Chiefs of Staff Instruction 6211.02D
Defense Information System Network (DISN) Responsibilities

Chairman of the Joint Chiefs of Staff Instruction 6510.01F
Information Assurance and Support to Computer Network Defense

Chairman of the Joint Chiefs of Staff Manual 6510.01B
Cyber Incident Handling Program

Committee on National Security Systems Directive No. 901
Committee on National Security Systems (CNSS) Issuance System (Available at https://www.cnss.gov/CNSS/issuances/Issuances.cfm.)

Committee on National Security Systems Instruction No. 4009
National Information Assurance (IA) Glossary (Available at https://www.cnss.gov/CNSS/issuances/Issuances.cfm.)

DA Pam 40–11
Preventive Medicine

DA Pam 525–27
Army Emergency Management Program

DA Pam 600–24
Health Promotion, Risk Reduction, and Suicide Prevention

DOD 3020.45, Volume 1
Defense Critical Infrastructure Program (DCIP): DOD Mission-Based Critical Asset Identification Process (CAIP)

DOD 3020.45, Volume 2
Defense Critical Infrastructure Program (DCIP): DCIP Remediation Planning

DOD 3020.45–M, Volume 3
Defense Critical Infrastructure Program (DCIP): Security Classification Manual (SCM)

DOD 3020.45, Volume 5
Defense Critical Infrastructure Program (DCIP): Execution Timeline

DOD 5200.08–R
Physical Security Program

DOD 5205.02–M
DOD Operations Security (OPSEC) Program Manual

DOD 5240.1–R
Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons

DOD DTM 09–012
Interim Policy Guidance for DOD Physical Access Control

DODD 3020.26
Department of Defense Continuity Programs

DODD 3020.40
DOD Policy and Responsibilities for Critical Infrastructure

DODD 5200.27
Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense

DODD 5210.88
Safeguarding Biological Select Agents and Toxins (BSAT)

DODD 5230.11
Disclosure of Classified Military Information to Foreign Governments and International Organizations

DODD 5240.01
DOD Intelligence Activities

DODD 5525.4
Enforcement of State Traffic Laws on DOD Installations

DODD 6490.02E
Comprehensive Health Surveillance

DODD 8500.01E
Information Assurance (IA)

DODI O–5210.63
DOD Procedures for Security of Nuclear Reactors and Special Nuclear Materials (SNM)

DODI 1000.29
DOD Civil Liberties Program

DODI 2000.12
DOD Antiterrorism Program

DODI 2000.16
DOD Antiterrorism (AT) Standards

DODI 3020.42
Defense Continuity Plan Development

DODI 3020.45
Defense Critical Infrastructure Program (DCIP) Management

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 5210.65
Minimum Security Standards for Safeguarding Chemical Agents

DODI 5240.04
Counterintelligence (CI) Investigations

DODI 5525.09
Compliance of DOD Members, Employees, and Family Members Outside the United States With Court Orders

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 Installation Emergency Management (IEM) Program

DODI 6200.03
Public Health Emergency Management within the Department of Defense

DODI 6490.03
Deployment Health

DODI O–2000.22
Designation and Physical Protection of DOD High Risk Personnel (HRP)

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 Classified Information

DODM 5200.01, Volume 3
DOD Information Security Program: Protection of Classified Information

DODM 5200.01, Volume 4
DOD Information Security Program: Controlled Unclassified Information (CUI)

Federal Emergency Management Agency, Independent Study Guide S–319
Exercise Design (Available at http://training.fema.gov/.)

FM 3–37.2
Antiterrorism

FM 4–02
Army Health System

FM 4–02.17
Preventive Medicine Services

FM 5–19
Composite Risk Management

General Order 2012–01
Assignment of Functions and Responsibilities within Headquarters, Department of the Army

Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors
Policy for a Common Identification Standard for Federal Employees and Contractors (Available at http://www.dhs.gov/homeland-security-presidential-directive-12.)

JP 1–02
Department of Defense Dictionary of Military and Associated Terms

JP 3–0
Joint Operations

JP 3–07.2
Antiterrorism

JP 3–13
Information Operations

JP 3–33
Joint Task Force Headquarters

JP 3–34
Joint Engineer Operations

JP 5–0
Joint Operations Planning

National Defense Authorization Act (NDAA) 2008, Section 1069
Standards Required for Entry for Installations in the United States (Available at http://www.gpo.gov/fdsys/pkg/PLAW–110publ181/html/PLAW–110publ181.htm.)

National Security Presidential Directive–51 / Homeland Security Presidential Directive–20
(Available at http://georgewbush-whitehouse.archives.gov/news/releases/2007/05/20070509–12.html.)

Presidential Memorandum — National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs
(Available at http://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 http://www.gpo.gov/fdsys/search/home.action.)

Public Law 110–53
Implementing Recommendations of the 9/11 Commission Act of 2007 (Available at http://www.gpo.gov/fdsys/search/home.action.)

Title 10, United States Code, Section 3013
Secretary of the Army (Available at http://www.gpo.gov/fdsys/search/home.action.)

Title 50, United States Code, Section 797
Penalty for Violation of Security Regulations and Orders (Available at http://www.gpo.gov/fdsys/search/home.action.)

UFC 3–340–01
Design and Analysis of Hardened Structures to Conventional Weapons Effects

UFC 3–340–02
Structures to Resist the Effects of Accidental Explosions

UFC 4–010–01
DOD Minimum Antiterrorism Standards for Buildings

UFC 4–010–02
DOD Minimum Antiterrorism Standoff Distances for Buildings

UFC 4–010–03
Security Engineering: Physical Security Measures for High-Risk Personnel

UFC 4–010–05
Sensitive Compartmented Information Facilities Planning, Design, and Construction

UFC 4–020–01
DOD Security Engineering Facilities Planning Manual

UFC 4–020–02FA
Security Engineering: Concept Design

UFC 4–020–03FA
Security Engineering: Final Design

UFC 4–021–01
Design and O&M: Mass Notification Systems

UFC 4–021–02
Electronic Security Systems

UFC 4–022–01
Security Engineering: Entry Control Facilities / Access Control Points

UFC 4–022–02
Selection and Application of Vehicle Barriers

UFC 4–022–03
Security Fences and Gates

UFC 4–023–03
Design of Buildings to Resist Progressive Collapse

UFC 4–024–01
Security Engineering: Procedures for Designing Airborne Chemical, Biological, and Radiological Protection for Buildings

UFC 4–025–01
Security Engineering: Waterfront Security

Section III
Prescribed Forms
This section contains no entries.

Section IV
Referenced Forms
Except where otherwise indicated below, the following forms are available as follows: DA Forms are available on the APD Web site at http://www.apd.army.mil.

DA Form 11–2
Internal Control Evaluation Certification

DA Form 2028
Recommended Changes to Publications and Blank Forms

Appendix B
The Army Protection Program Functional Elements and Enabling Functions

B–1. Army Protection Program functional elements
This section briefly defines and identifies the Army proponent and the primary references for the APP functional elements. Additional references for each of the APP functional elements are found in appendix A.

a. Antiterrorism.

(1) AT is defined as 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.

(2) Army proponent: The PMG is the proponent for AT Program in direct support to the HQDA, DCS, G–3/5/7 for the management and execution of the Army AT mission.

(3) Primary reference: AR 525–13.

(4) Supporting references: Field Manual (FM) 3–37.2, DODI 2000.12, DODI 2000.16, and Joint Publication 3.07–2.

b. Computer Network Defense.

(1) CND is defined as actions taken to protect, monitor, analyze, defend, and respond against unauthorized activity within Army and/or DOD information systems and computer networks. CND actions include protection, monitoring, analysis, detection, response (to include restoration), and capability sustainment. Commanders of ACOMs, ASCCs, and DRUs; CNGB; CAR; and direct reporting program managers responsibilities include ensuring their units, activities, and installations develop and implement an IA program to support Army CND efforts.

(2) Army proponent: ARCYBER is the designated CND service provider and provides top-level direction and coordination to CND elements and/or operations at commands, installations, and stand-alone facilities.

(3) Primary reference: AR 25–2.

(4) Supporting references: AR 25–1, AR 195–2, AR 380–5, AR 380–53, AR 380–381, and Chairman of the Joint Chiefs of Staff Manual 6510.01B.

c. Continuity of Operations Program.

(1) COOP is defined as policies, plans, procedures, and capabilities that provide for the continued execution of critical missions and functions across a wide range of potential emergencies, including localized acts of nature, accidents, technological, and/or attack related emergencies. The COOP responsibilities of commanders of ACOMs, ASCCs, and DRUs include developing and maintaining a COOP program and maintaining a COOP operations plan (OPLAN) that identifies and prioritizes MEFs.

(2) Army proponent: The DCS, G–3/5/7 is the DA proponent for COOP.

(3) Primary reference: AR 500–3.

(4) Supporting references: Department of Defense Directive (DODD) 3020.26, DODI 3020.42, and National Security Presidential Directive-51/Homeland Security Presidential Directive-20.

d. Critical Infrastructure Risk Management.

(1) CIRM is the Army program to implement Defense Critical Infrastructure Program responsibilities by conducting the Critical Asset Identification Process with ACOMs, ASCCs, and DRUs; USAR; and ARNG to identify Task Critical Assets; nominate Defense Critical Assets; and conduct risk management activities. The CIRM responsibilities of the commanders of ACOMs, ASCCs, and DRUs; USAR; and ARNG include maintaining awareness of infrastructure risk and implementing required risk mitigation strategies.

(2) Army proponent: The DCS, G–3/5/7 is the Army's Critical Infrastructure Assurance Officer.

(3) Primary reference: AR 525–26.

(4) Supporting references: DODD 3020.40; DODI 3020.45; DOD 3020.45, Volume 1; DOD 3020.45, Volume 2; DOD 3020.45–M, Volume 3; and DOD 3020.45, Volume 5.

e. Emergency Management.

(1) The EM function serves as the single, comprehensive, and integrated EM program on Army installations, facilities, and activities. 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 (man-made), and terrorism hazards. The EM responsibilities of senior commanders include 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 DA 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.

f. Fire and Emergency Services.

(1) F&ES is defined as the program that ensures public safety by providing response capabilities and medical services during emergencies. The F&ES Program provides 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, and family members, and of an expeditionary Army in a time of persistent conflict.

(2) Army proponent: The ACSIM is the DA proponent for the F&ES Program.

(3) Primary reference: AR 420–1.

(4) Supporting reference: DODI 6055.06.

g. Health Protection.

(1) HP is defined as 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. HP 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 proponent: The Surgeon General is the DA proponent for HP.

(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 (ADRP 4–0), FM 4–02, FM 4–02.17, DODD 6490.02E, and DODI 6490.03.

h. High-risk personnel.

(1) Senior Army civilian and military leadership serve as an extended symbol of our nation's Army, making them attractive and accessible targets. Some personnel are at a greater risk than the general population by virtue of their rank, assignment, symbolic value, vulnerabilities, location, or a specific threat requiring additional security to reduce or eliminate risk. These individuals are formally designated as HRP. Additional protection may be provided to HRP through progressive levels of training, equipment support, facilities improvement, and/or personnel protective services detail support.

(2) Army proponent: The PMG is the proponent for the security of personnel which includes HRP designation and protection. The USACIDC plans for and provides personal security (protective services) for designated DOD, DA HRP, and foreign officials as directed. The DCS, G–3/5/7 is responsible for the security of the Army and provides overall policy guidance and staff supervision and coordination for the Army Force Protection and AT programs. The PMG is in direct support to the DCS, G–3/5/7 for the management and execution of the Army AT mission. The USACIDC is responsible for planning and coordinating the protection of HRP for DOD, DA, and foreign officials as directed by HQDA.

(3) Primary references: Department of Defense Instruction (DODI) O–2000.22, AR 190–58, and AR 525–13.

i. Information Assurance.

(1) The IA Program is the protection of systems and information in storage, processing, or transit from unauthorized access or modification; denial of service to unauthorized users; or the provision of service to authorized users. It includes those measures necessary to detect, document, and counter such threats. Measures that protect and defend information and information systems (IS) ensure their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of IS by incorporating protection, detection, and reaction capabilities. Commanders of ACOMs, ASCCs, and DRUs; ARNG; and USAR; program evaluation offices (PEOs); and direct reporting program managers (PMs) responsibilities for IA include ensuring their units, activities, or installations develop and implement an IA program with hardware, software, tools, personnel, and infrastructure.

(2) Army proponent: The CIO/G–6 establishes and issues IA policy and procedures, and is the focal point for the IA Program.

(3) Primary references: AR 25–2 and Committee on National Security Systems Instruction No. 4009.

(4) Supporting references: AR 25–1, AR 380–5, AR 380–53, AR 380–381, Chairman of the Joint Chiefs of Staff Instruction 6211.02D, Chairman of the Joint Chiefs of Staff Instruction 6510.01F, Chairman of the Joint Chiefs of Staff Instruction Manual 6510.01B, Joint Publication 3–13, DODD 8500.01E, DOD Manual 5200.01, Volumes 1–4, and Committee on National Security Systems Directive No. 901.

j. Law Enforcement.

(1) LE is defined as 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) Army proponent: The PMG establishes and develops policies and procedures for Army LE.

(3) Primary references: AR 190–30 and AR 190–45.

(4) 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, ATTP 3–39.20, DODD 5525.4, DODD 5525.5, DODI 5200.8, DODI 5240.4, DODI 5525.09, and DODI 5525.15.

k. Operations Security.

(1) OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: identify those actions that can be observed by adversary intelligence systems; determine indicators that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. 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: DOD Manual 5205.02–M.

l. Physical Security.

(1) The PS Program is defined as 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 prescribes policies for 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 prescribes policies for the protection of Army sites, specifically controlling access to installations and stand-alone facilities and restricted area controls. The program also prescribes policies for Army civilian police and security guards. The commanders and directors of ACOMs, ASCCs, DRUs, USAR, and ARNG PS responsibilities include establishing a PS program to plan and coordinate PS matters.

(2) Army proponent: The PMG is responsible for the Army PS Program.

(3) Primary reference: AR 190–13.

(4) Supporting references: ADP 3–37; ADRP 3–37; AR 190–11; AR 190–17; AR 190–51; AR 190–54; AR 190–56; AR 190–59; ATTP 3–39.32; DOD Directive-Type Memorandum 09–012; DODD 5210.88; DODI 5200.8; DODI 5210. 65; DODD O–5210.63; DOD Manual 5100.76M; DOD Regulation 5200.8R; Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors; National Defense Authorization Act (NDAA) 2008, Section 1069; and Title 50, United States Code, Section 797.

B–2. Army Protection Program enabling functions

This section briefly defines and identifies the Army proponent, and identifies the primary references for the APP enabling functions. Additional references for each of the APP enabling functions are found in appendix A.

a. Intelligence and Counterintelligence.

(1) Intelligence and CI intelligence 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 detect and mitigate threats posed by trusted insiders, and helps protect classified and other protected information from loss, compromise, or unauthorized disclosure. Army CI and security 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 classified information security, personnel security, industrial security, communications security (COMSEC), 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 security support to technology protection.

(2) 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 such as insider threats, that threaten the survivability and mission accomplishment of military personnel, civilian employees, family members, contractors and units.

(3) 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 decisionmaking. 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.

(4) Army proponents:

(a) The DCS, G–2 has Army Staff responsibility for overall coordination of the five major intelligence disciplines: Imagery Intelligence, Signals Intelligence, Human Intelligence, Measurement and Signature Intelligence, and CI and Security Countermeasures.

(b) The USACIDC provides CRIMINT SME related to personal 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.

(5) Primary references include: AR 381–10, AR 381–12, AR 381–20, and AR 195–2.

(6) Supporting references include: AD 2013–18, 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, and Presidential Memorandum — National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs.

b. Security Engineering.

(1) SE services assist in protecting designated assets against criminal and terrorist threats, and military weapons effects. SE 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. SE 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 proponent: The USACE Protective Design Center develops and maintains security engineering construction codes and provides SE services.

(3) Primary references: The Unified Facilities Criteria (UFC) series of documents, identified in appendix A of this regulation.

Appendix C
Army Protection Program Management Structure 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 principal officials.

(3) Coordinates and integrates the APP functional elements 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 elements.

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.

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) ASA (FM&C).
(4) ASA (IE&E).
(5) ASA (ALT).
(6) General Counsel.
(7) Director of the Army Staff.
(8) Administrative Assistant to the Secretary of the Army.
(9) CIO/G–6.
(10) DARNG.
(11) DCS, G–1.
(12) DCS, G–2.
(13) DCS, G–4.
(14) DCS, G–8.
(15) CAR.
(16) Chief of Engineers.
(17) The Surgeon General.
(18) ACSIM.
(19) The Judge Advocate General.
(20) Chief of Chaplains.
(21) The PMG.

f. Proxy and advisory capacity. When the above principal officials 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 (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) ASA (M&RA).
(4) ASA (FM&C).
(5) ASA (IE&E).
(6) ASA (ALT).
(7) General Counsel.
(8) Administrative Assistant to the Secretary of the Army.
(9) Chief Information Officer/G–6.
(10) DARNG.
(11) Director of the Army Staff.
(12) DCS, G–1.
(13) DCS, G–2.
(14) DCS, G–4.
(15) DCS, G–8.
(16) CAR.
(17) Chief of Engineers.
(18) The Surgeon General.
(19) ACSIM.
(20) The Judge Advocate General.
(21) Chief of Chaplains.

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 quarterly.

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

Appendix D
Base Integrated Protection Plan Format for Commands, Agencies, and Activities.

See chapter 5 for applicable organizations and requirements. Some sections may be classified.

D–1. Base integrated protection plan

a. Date of update. (Updated annually.)

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 functional elements and their associated enabling functions within the command's operations-focused organization (or G–34) 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 functional elements 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 in appendix B 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, training events, and exercises. Address the consolidated and integrated annual full-scale protection exercise and identify the capabilities from multiple APP functional elements and the command and control capabilities that will be exercised in the current year, and the schedule for exercising all APP functional elements at least triennially (such as tabletop, functional, and/or full-scale).

h. Approving signature of senior commander or leader.

D–2. Appendix A — 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. Appendix B — 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. Appendix C — Directory of Army Protection Program functional elements 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)'s, installation(s)', and stand-alone facilities' protection functions and emergency operations center(s) phone numbers and email directories.

D–5. Appendix D — 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. Appendix E — 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. Appendix F — 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 decisionmaking 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. Example of threats and hazards could include: active shooters, hazardous material spills, cyber attacks and denial of services, utility disruptions, extreme weather events, pandemic events, events that requires relocation and activation of COOPs at each applicable installation and separate 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; CAR; Chief, National Guard Bureau; 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 five (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 quarterly 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 monthly APPCOC with the appropriate (colonel or equivalent) level of representation?

(4) Has the DCS, G–3/5/7 developed and disseminated to the ACOMs, ASCCs, and DRUs; USAR; CNGB; agencies and activities; and senior commanders of garrisons 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?

(5) Have ACOMs, ASCCs, DRUs, USAR, CNGB, agencies and activities, and senior commanders of garrisons, established a PEC as the single, overarching protection forum to integrate and coordinate all APP functional elements and enabling functions?

(6) Have ACOMs, ASCCs, DRUs, USAR, CNGB, agencies and activities, and senior commanders of garrisons synchronized, integrated, and coordinated the APP functional elements and enabling functions and focused protection efforts on the Command's, the Army's, and DOD's MEFs and operational requirements, within the operations (G–34 or similar) section of the organization?

(7) Are ACOMs, ASCCs, DRUs, USAR, CNGB, agencies and activities, and senior 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 and 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?

b. Assessments.

(1) Are HQDA SMEs from the APP functional elements and their associated enabling functions conducting triennial APPAs?

(2) Are corrective actions from ACOMs, ASCCs, DRUs, USAR, CNGB, agencies and activities APPAs and associated RBEs being tracked and addressed at semi-annual observation resolution boards?

(3) Are ACOMs, ASCCs, DRUs, USAR, CNGB, agencies and activities utilizing APP functional elements and the associated enabling functions SMEs to conduct tailored integrated higher headquarters protection assessments (HHPA) of their subordinate commands, a minimum of triennially?

(4) Are ACOMs, ASCCs, DRUs, USAR, CNGB, agencies and activities, forwarding trend analysis of subordinate commands' HHPAs twice a year to the HQDA, DCS G–3/5/7 (G–34) for programmatic analysis and to facilitate the efficient and effective PPBE of protection-related resources to meet identified Army requirements?

(5) 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 (G–34)?

c. Exercises.

(1) Are ACOMs, ASCCs, DRUs, USAR, CNGB, agencies and activities publishing an annual execution order for the fiscal year outlining the commands' APP priorities and integrated APP exercises for subordinate commands?

(2) Are senior commanders and leaders at installations and stand-alone facilities planning and conducting an annual consolidated and integrated protection exercise that includes capabilities from multiple APP functional elements, and evaluates APP command and control capabilities for the protection elements that are within their sphere of control and influence?

(3) Are senior commanders and leaders at installations and stand-alone facilities ensuring multiple APP functional elements and command and control capabilities for the protection elements are exercised and evaluated every year, and triennially conducting an exercise (such as tabletop, functional, and/or full scale) that evaluates the capabilities of all the APP functional elements?

E–5. Supersession

Not applicable.

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

ACSIM
Assistant Chief of Staff for Installation Management

ACOM
Army Command

ADRP
Army doctrine reference publication

APP
Army Protection Program

APPL
Army Prioritized Protection List

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

ATTP
Army tactics, techniques, and procedures

CAR
Chief, Army Reserve

CAT
Crisis Action Team

CG
Commanding General

CI
Counterintelligence

CIO/G–6
Chief Information Officer, G–6

CIRM
Critical Infrastructure Risk Management

CND
Computer Network Defense

CNGB
Chief, National Guard Bureau

COE
Chief of Engineers

COMSEC
Communications Security

COOP
Continuity of Operations

DA
Department of the Army

DAS
Director of the Army Staff

DARNG
Director, Army National Guard

DCS, G–1
Deputy Chief of Staff, G–1

DCS, G–2
Deputy Chief of Staff, G–2

DCS, G–3/5/7
Deputy Chief of Staff, G–3/5/7

DCS, G–4
Deputy Chief of Staff, G–4

DCS, G–8
Deputy Chief of Staff, G–8

DOD
Department of Defense

DODD
Department of Defense Directive

DODI
Department of Defense Instruction

DOTMLPF
doctrine, organization, training, materiel, leadership and education, personnel and facilities

DRU
direct reporting unit

EM
emergency management

F&ES
Fire and Emergency Services

FM
field manual

GCC
geographic combatant commands

GIS
geographic information system

HQDA
Headquarters, Department of the Army

HRP
high-risk personnel

IA
information assurance

IG
Inspector General

IS
information system

ISR
installation status report

ISSA
inter-Service support agreement

JPEO
Joint Program Executive Office

JS
Joint Staff

LE
law enforcement

MAA
mutual aid agreement

MDEP
management decision package

MEF
mission essential function

MOA
memorandum of agreement

MOU
memorandum of understanding

NGO
non-governmental organization

OCAR
Office of the Chief, Army Reserve

OIP
Organizational Inspection Program

OPLAN
operations plan

OPMG
Office of the Provost Marshal General

OPSEC
operations security

OSD
Office of the Secretary of Defense

PEC
Protection Executive Committee

PEG
Program Evaluation Group

PEO
Program Executive Office

PM
program manager

PMG
Provost Marshal General

POM
program objective memorandum

PPBE
planning, programming, budgeting and execution

PS
physical security

RBE
reply by endorsement

RMD
Resource Management Directive

SME
subject matter expert

TAP
The Army Plan

TEMPEST
Telecommunications Electronics Materiel Protected from Emanating Spurious Transmissions

TRADOC
U.S. Army Training and Doctrine Command

TSG
The Surgeon General

UFC
Unified Facilities Criteria

USACE
U.S. Army Corps of Engineers

USACIDC
U.S. Army Criminal Investigation Command

USAR
United States Army Reserve

USR
unit status report

Section II
Terms

All-hazards
Any incident, natural or manmade (including those defined in DODI 6055.07, Mishap Notification, Investigation, Reporting, and Record Keeping) that warrants action to protect the life, property, health, and safety of military members, dependents, and civilians at risk, and minimize any disruptions of installation operations. (DODI 6055.17)

Army Protection Program
The over-arching leadership framework to integrate, coordinate, synchronize, and prioritize protection policies and resources among the functional elements and the associated enabling functions.

Army Prioritized Protection List
A prioritization tool that provides a source list of installations that are rank ordered utilizing an objective methodology that accounts for various factors including, but not limited to, standard garrison organization inputs, strategic functionality and criticality, and threat.

Computer Network Defense
Actions taken to defend against unauthorized activity within computer networks. Computer Network Defense includes monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities. (Committee on National Security Systems Instruction No. 4009)

Continuity of Operations
The degree or state of being continuous in the conduct of functions, tasks, or duties necessary to accomplish a military action or mission in carrying out national military strategy. It includes the functions and duties performed by the commander, his or her staff, and others acting under the authority and direction of the commander. (AR 500–3)

Critical asset
A specific entity that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of a nation to continue to function effectively. (Joint Publication 3–07.2)

Cybersecurity
The ability to protect or defend the use of cyberspace from cyber attacks. (Committee on National Security Systems Instruction No. 4009)

Defense critical asset
An asset of such extraordinary importance to operations in peace, crisis, and war that its incapacitation or destruction would have a very serious, debilitating effect on the ability of the Department of Defense to fulfill its missions. (DODD 3020.40)

Defense critical infrastructure
The composite DOD and non-DOD assets essential to project, support, and sustain military forces and operations worldwide. DCI is a combination of task critical assets and defense critical assets. (DODD 3020.40)

Defense Critical Infrastructure Program
A DOD risk management program that seeks to ensure the availability of Defense Critical Infrastructure. (DODD 3020. 40)

Facility
A real property entity consisting of one or more of the following: a building, a structure, a utility system, pavement, and underlying land. (Joint Publication 3–34)

Full-scale exercise
An exercise that simulates a real event as closely as possible, designed to evaluate integrated capabilities in a highly stressful environment that simulates actual conditions. It is a lengthy exercise which requires the mobilization and actual movement of personnel, equipment, and resources that would be called upon in a real event, taking place on location in an environment as near to real as possible. It tests capabilities, exercises most functions, must coordinate the efforts of several organizations, and the Emergency Operations Center must be activated. (Derived from the Federal Emergency Management Agency's Exercise Design course, IS–319, Unit 7: The Full-Scale Exercise; DA Pam 527–27; and DODI 6055.17.)

Hazard
(1) A condition with the potential to cause injury, illness, or death of personnel; damage to or loss of equipment or property; or mission degradation. See also injury; risk (Joint Publication 3–33). (2) Something that is potentially dangerous or harmful (AR 525–27). (3) A condition with the potential of injuring personnel, damaging equipment or structures, losing material, or reducing the ability to perform a prescribed function (AR 525–26).

Health protection
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.

High-risk personnel
(1) Personnel who, by their grade, assignment, symbolic value, or relative isolation, are likely to be attractive or accessible terrorist targets (AR 525–13). (2) Personnel who are more likely to be terrorist or criminal targets because of their grade, assignment, symbolic value, vulnerabilities, location, or specific threat (AR 190–58).

Incident
(1) An occurrence or event, natural or manmade that requires a response to protect life or property. Incidents can, for example, include major disasters, emergencies, terrorist attacks, terrorist threats, civil unrest, wild land and urban fires, floods, hazardous material spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, tsunamis, war-related disasters, medical and public health emergencies, and other occurrences requiring an emergency response (DODI 6055.17). (2) An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies (Committee on National Security Systems Instruction No. 4009).

Information assurance
Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation, which includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (Joint Publication 3–33, Committee on National Security Systems Instruction No. 4009)

Insider threat
(1) The threat that an insider will use her/his access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through loss or degradation of departmental resources or capabilities (National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs). (2) A person with placement and access who intentionally causes loss or degradation of resources or capabilities or compromises the ability of an organization to accomplish its mission through espionage, providing support to international terrorism, or the unauthorized release or disclosure of information about the plans and intentions of U.S. military forces (AR 381–20).

Installation
An aggregation of contiguous or near contiguous, common mission-supporting real property holdings under the control and jurisdiction of DOD, and at which, an Army unit or activity is permanently assigned. For the purpose of Army EM installation is used collectively to include all Army installations, facilities, and/or activities. (AR 525–27)

Mission assurance
A process to protect or ensure the continued function and resilience of capabilities and assets—including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains—critical to the execution of DOD mission-essential functions in any operating environment or condition. (DODD 3020.40)

Mission essential function
(1) Any function that is vital to the continuation of operations of the organization or agency. These functions include those required by statute or Executive Order, and other functions deemed essential by the head of each organization. MEFs are those continuing activities that must be performed without interruption to execute critical Army missions. MEFs may be prioritized, which allows for a graduated response and relocation to the Emergency Relocation Facilities with minimum interruptions to operations during a national/local emergency or during normal operations (AR 500–3). (2) The specified or implied tasks required to be performed by, or derived from, statute, Executive order, or other appropriate guidance, and those organizational activities that must be performed under all circumstances to achieve DOD component missions or responsibilities in a continuity threat or event. Failure to perform or sustain these functions would significantly affect the Department of Defense's ability to provide vital services or exercise authority, direction, and control (DODD 3020.26).

Mission essential task
A mission task selected by a commander deemed essential to mission accomplishment and defined using the common language of the universal joint task list in terms of task, condition, and standard. Differs from a joint mission essential task in that it may reflect missions task within a sole DOD Component's authority. (DOD Manual 3020.45–V1)

Protection
For the purposes of this regulation, "Protection" is defined as the preservation of 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 hazards environment.

Resiliency
The characteristic or capability to maintain functionality and structure (or degrade gracefully) in the face of internal and external change. (DODI 3020.45)

Risk
Probability and severity of loss linked to threats or hazards and vulnerabilities. (Joint Publication 5–0)

Risk assessment
A systematic examination of risk using disciplined processes, methods, and tools. A risk assessment provides an environment for decision makers to evaluate and prioritize risks continuously and to recommend strategies to remediate or mitigate those risks. (DODD 3020.40)

Risk management
(1) A continual process or cycle where risks are identified, measured, and evaluated; countermeasures are then designed, implemented, and monitored to see how they perform, with a continual feedback loop for decision-maker input to improve countermeasures and consider tradeoffs between risk acceptance and risk avoidance (DODI 6055.17). (2) The process of identifying, assessing, and controlling risks arising from operational factors and making decisions that balance risk cost with mission benefits (Joint Publication 3–0).

Security resiliency
An initiative to significantly reduce the risk of insider incidents by synchronizing counterintelligence, security, force protection, LE, and cyber efforts.

Senior Commander
Command of Army installations is exercised by a senior commander (SC). The SC is designated by senior Army leadership. The SC's command authority over the installation derives from the Chief of Staff, Army (CSA) and Secretary of the Army's (SA) authority over installations. This is a direct delegation of command authority for the

installation to the SC. The SC's command authority includes all authorities inherent in command including the authority to ensure the maintenance of good order and discipline for the installation. (AR 600–20; AR 525–27)

Task critical asset
An asset that is of such extraordinary importance that its incapacitation or destruction would have a serious, debilitating effect on the ability of one or more DOD component or Defense Infrastructure Sector Lead Agents organizations to execute the task or mission essential task it supports. Task critical assets are used to identify defense critical assets. (DODD 3020.40)

Terrorism
The calculated use of unlawful violence or threat of unlawful violence to inculcate fear, intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological. (Joint Publication 1–02)

Threat
An adversary having the intent, capability, and opportunity to cause loss or damage. (DODD 3020.40)

Vulnerability assessment
(1) A systematic examination of the characteristics of an installation, system, asset, application, or its dependencies to identify vulnerabilities (DODD 3020.40). (2) A DOD, command, or unit-level evaluation (assessment) to determine the vulnerability of a terrorist attack against an installation, unit, exercise, port, ship, residence, facility, or other site. Identifies areas of improvement to withstand, mitigate, or deter acts of violence or terrorism (Joint Publication 3–07.2).

Section III
Special Abbreviations and Terms

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

ARTIC
Army Threat Integration Center

CRIMINT
Criminal intelligence

HHPA
High headquarters protection assessment

HP
Health Protection

IPP
Integrated protection plan

MARMS
Mission Assurance Risk Management System

MAVNI
Military accessions vital to national interest

PPBC
Planning, Programming, Budgeting Committee

PTWG
Protection threat working group

PWG
Protection working group

SE
Security engineering