DEPARTMENT OF THE ARMY
U.S. ARMY INSTALLATION MANAGEMENT COMMAND
HEADQUARTERS, UNITED STATES ARMY GARRISON WEST POINT
681 ROGERS PLACE
WEST POINT, NEW YORK 10996-1514

AMIM-MLG-ZA (381-3a) 1 May 2026

U.S. ARMY GARRISON WEST POINT POLICY #23

SUBJECT: Operations Security (OPSEC) Plan for USAG West Point

1. Applicability. This plan applies to all USAG West Point military, DOD Civilian, and contractor personnel. Tenant units are encouraged to adopt this plan into their command plans.

2. Purpose. The purpose of this plan is to establish and maintain the USAG West Point OPSEC Program as set forth in National Security Decision Directive 298, Chairman, Joint Chiefs of Staff Instruction (CJCSI) 3213.01C, Joint Publication (JP) 3-13.3, Department of Defense Directive 5205.02, and Operations Security, Army Regulation 530-1. The plan will be reviewed annually and updated as required.

a. As a Commander's program, OPSEC is a required process for all missions within the USAG West Point Area of Operations (AO) including day-to-day operations, planning, training, special events, and other ceremonies. Additionally, this OPSEC Plan will:

(1) Assign OPSEC responsibilities.

(2) Identify requirements to plan for and implement OPSEC.

(3) Define a systematic approach to developing necessary OPSEC measures.

(4) Specify USAG West Point-wide OPSEC training.

(5) Provide review requirements for USAG West Point OPSEC measures and reporting.

(6) Describe cross-command and interagency support of the OPSEC program, which includes assessments and survey training.

(7) Ensure OPSEC reviews are included in Logistic Contracts and subcontract requirements.

b. Requirements for OPSEC. Secrecy and safeguarding of information, such as friendly intentions, capabilities, planning, and execution data is important to the OPSEC

process. Compartmentalization to accomplish such secrecy and safeguarding is not encouraged except in extreme cases.

3. USAG West Point Mission Statements.

a. Mission: Provide premium base Installation services to our military community and its stakeholders while supporting accession and Defense Support to Civil Authorities in the New York area.

b. Vision: Transform to a self-sustaining installation while providing the best customer service in the eyes of our military members, stakeholders, tenant units and families.

4. Responsibilities. OPSEC is everyone's responsibility.

a. USAG West Point Commander’s Responsibilities.

(1) For issuing orders, directives, and policies to protect the command’s critical and sensitive information to clearly define the specific OPSEC measures all command personnel should practice.

(2) Ensuring that USAG West Point’s OPSEC program and OPSEC measures are coordinated and synchronized with the higher command’s security programs such as information security (INFOSEC), information assurance (IA), physical security (PS), force protection (FP), and so forth.

(3) Ensuring all USAG West Point official information released to the public, to include the World Wide Web, receives an OPSEC review prior to dissemination.

(4) Establishing a documented OPSEC program that includes as a minimum, OPSEC Officer Appointment orders and an OPSEC program document.

(5) Appointing an OPM/officer in writing with responsibility for supervising the execution of the OPSEC program within the organization.

(6) Ensuring that the appointed OPSEC Officer receives required training in accordance with regulatory guidance.

(7) Approving the USAG West Point’s Critical Information List (CIL). Distribute the list to USAG West Point service members, DOD Civilians and contractors.

(8) Providing guidance and direction to ensure that the Garrison understands, adapts and applies the CIL to that organization’s mission and provides feedback to the commander.

(9) Weighing the risks to the mission against the costs of protection and decide what OPSEC measures to implement. Publish these measures in all Operations Plans (OPLANs) and Operations Orders (OPORDs) or in an OPSEC plan.

b. Directorate of Plans, Training, Mobilization, and Security (DPTMS/G3) will:

(1) Serve as the USAG West Point's principal staff officer for overall management of the OPSEC program. The DPTMS is the proponent for OPSEC, but the entire staff must integrate OPSEC into planning and execution of the organization's missions.

(2) Appoint an OPM to manage and oversee the implementation of the Command OPSEC Program and ensure that OPSEC is integrated with law enforcement sensitive and other security operations that are critical to the command and its missions.

(3) Ensure the integration and synchronization of the USAG West Point's OPSEC program with higher headquarters OPSEC program.

c. Command OPSEC Manager/Officer (OPM-G3) will:

(1) Publish a West Point OPSEC Plan that establishes minimum standards for conducting OPSEC missions within the Area of Operations.

(2) Be appointed in writing as the Command OPM.

(3) Oversee the implementation of the OPSEC program throughout West Point.

(4) Interpret OPSEC policies of senior authorities, prepare and recommend OPSEC policies. Provide OPSEC guidance to command group and staff members.

(5) Ensure the OPSEC program conforms to pertinent policies of higher authorities. When required, recommend changes to the policies of higher authorities.

(6) Produce OPSEC Appendices or Annexes for OPLANs or OPORDs to Plans and OPORDs.

(7) Ensure OPSEC measures are included in all USAG West Point contracts and subcontracts to protect critical or sensitive information.

(8) Ensure OPSEC reviews are conducted on all USAG West Point contracts and subcontract documents such as a Request for Proposal (RFP) or Statement of Work (SOW).

(9) Maintain awareness of all organizational missions and advise required personnel concerning the OPSEC posture of these missions.

(10) Ensure OPSEC training is conducted in accordance with DOD 5205.2, AR 530-1 and this OPSEC Plan.

(11) Represent the command on OPSEC matters. Attend OPSEC conferences, training sessions, and briefings.

(12) Integrate intelligence, counterintelligence, Force Protection, and Information Operations (IO) into OPSEC planning and practice as required.

(13) Prepare and coordinate through the USAG West Point DPTMS and DES requests for intelligence and counterintelligence information for OPSEC planning, surveys and assessments.

(14) Conduct OPSEC reviews of operational plans and reports to ensure adherence to OPSEC policies and procedures.

(15) Support the Public Affairs Office mission regarding public disclosures.

(16) Support the USAG West Point PAO and NEC SharePoint Subject Matter Experts (SME) related to web postings.

(17) Support the Freedom of Information Act (FOIA) Officer related to information released under FOIA.

(18) Establish and chair the OWG or equivalent, at least quarterly.

(19) In conjunction with other OPSEC Coordinators/Officers input, develops the organization’s CIL.

(20) Develop and recommend OPSEC measures to be implemented within the Command.

(21) Conduct OPSEC assessments of subordinate units using the published OPSEC guidance to determine if the units are in compliance with regulatory guidance. The OPM/Coordinator must submit a written assessment with results and recommendations to the assessed organizations.

(22) Ensure training exercises include realistic OPSEC considerations. Ensure pre-exercise OPSEC briefings are conducted incorporating the threat, CIL, and OPSEC measures.

(23) Monitor the OPSEC programs of subordinate organizations by reviewing OPSEC plans/SOPs, survey results, exercise evaluations, and IG Reports.

(24) Conduct an annual OPSEC assessment.

(25) Be prepared to submit an annual OPSEC Program Report to the HQDA G-3/5/7 (G-39) NLT 15 December. The reporting period is from 1 October to 30 September of the prior fiscal year.

(26) Perform other duties and responsibilities IAW regulatory guidelines.

d. West Point OPSEC Working Group (OWG):

(1) Conduct an OWG or equivalent in accordance with DOD 5205.2, AR 530-1 and Annex C of this Plan.

(2) Develop an OWG or equivalent Charter for West Point Area Operations (AO).

(3) The OWG or equivalent should consist of USAG West Point, and tenant unit OPSEC Officers, and Coordinators.

(4) Conduct OPSEC meetings or equivalent, quarterly to:

(a) Provide policy oversight and review the USAG West Point OPSEC Program.

(b) Inform the Garrison Commander of the status of the OPSEC program.

(c) Highlight, explore, track, and discuss OPSEC challenges/issues.

(d) Identify and eliminate gaps and seams between higher headquarters and USAG West Point Policies and procedures.

(e) For economical use of resources, the OWG and the Antiterrorism Working Group (ATWG) will meet jointly.

e. West Point Tenant Commanders will:

(1) Develop and integrate their respective OPSEC programs using this publication.

(2) Develop and lead their Command OPSEC Programs down to lowest echelon level.

(3) Appoint in writing OPSEC Officers to manage the OPSEC Programs.

(4) Ensure OPSEC Officers conduct initial and annual OPSEC training.

(5) Establish and maintain an OPSEC Order, Plan or SOP and a CIL.

(6) Establish and chair OWG, semiannually.

(7) Ensure OPSEC Officers attend the West Point OWG, quarterly.

(8) Conduct periodic reviews to assess and maintain the effectiveness of the OPSEC program and OPSEC measures.

(9) Ensure OPSEC Annexes or Appendices are included in OPORDs and OPLANs for exercises, events, operational deployments and contingency support.

(10) Keep the USAG West Point Commander abreast of their OPSEC programs and provide advice and assistance to lower echelons.

(11) Maintain a Continuity Folder to be passed to the incoming OPSEC Officers. This will provide valuable information as to when the program was implemented and how it has progressed.

(12) Conduct an annual review of the OPSEC programs. The review will reflect the status of OPSEC programs each fiscal year and identify corrective measures to improve the programs or command awareness.

(a) Identify Primary and Alternate OPSEC Officer.

(b) Conduct overview of OPSEC program status.

(c) Monitor training and indoctrination program status.

(d) Any problem areas and recommendations for improvements.

(e) Report annually OPSEC program results and Lessons learned from incidents, exercises, or operations NLT 1 November of each fiscal year.

(f) Conduct an annual review of primary special staff, NIPRNET Home Pages and other applicable Web sites to ensure critical information is not inadvertently exposed.

(g) Ensure OPSEC measures are included in all USAG West Point contracts and subcontracts to protect critical or sensitive information and ensure OPSEC reviews are conducted on all USAG West Point contracts and subcontract documents such as a Request for Proposal (RFP) or Statements of Work (SOW).

(13) Provides annual reminders of the importance of sound OPSEC practices. These reminders consist of OPSEC news releases in command publications, OPSEC information bulletins, and OPSEC awareness briefings.

f. USAG West Point Directorates and Staff Elements will:

(1) Ensure required OPSEC measures are taken within their staffs/sections in order to provide maximum protection of all functions and missions.

(2) Assist the OPM with integrating OPSEC into all organizational missions.

(3) Ensure OPSEC Coordinators attend the USAG West Point OWG, quarterly.

(4) Ensure OPSEC measures are included in all USAG West Point contracts and subcontracts to protect critical or sensitive information and ensure OPSEC reviews are conducted on all USAG West Point contract and subcontract documents such as a Request for Proposal (RFP) or Statements of Work (SOW).

g. All USAG West Point personnel will:

(1) Implement OPSEC measures as determined by the USAG West Point Commander.

(2) Receive initial and annual OPSEC Level 1 awareness training.

(a) Become knowledgeable of USAG West Point Critical Information and how to protect it by applying OPSEC measures to prevent inadvertent disclosure

(b) Understand how OPSEC complements traditional security programs to maintain essential secrecy of U.S. military capabilities, intentions, and plans.

(c) Learn how to apply OPSEC to their daily tasks.

(d) Learn why OPSEC is important to the organization.

(e) Understand how adversaries aggressively seek information on U.S. military capabilities, intentions, and plans.

(f) Become knowledgeable of the local multidiscipline adversary intelligence threat.

(3) Practice need-to-know and telephone security.

(4) Limit distribution of rosters identifying personnel by position, military occupation specialty/area of responsibility, grade, and/or security clearance.

(5) Do not talk about work in public locations.

(6) Safeguard unclassified technical data.

(7) Be familiar with the OPSEC Program and where to obtain additional OPSEC guidance as needed.

(8) Actively encourage others, including Family members, Family readiness groups and Family support groups, to protect Critical Information.

(9) Handle any attempt by unauthorized personnel to solicit sensitive or critical information as a Threat Awareness Reporting Procedures (TARP) incident per AR 381-12.

(10) Report all attempts by unauthorized personnel to solicit sensitive or critical information immediately to the 1-800-CALL-SPY (24-hour nationwide hotline) and inform the chain of command.

5. Concept of Operations Security.

a. Operations Security (OPSEC). OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to:

(1) Identify those actions that can be observed by adversary intelligence systems.

(2) 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.

(3) Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

b. OPSEC Process. The OPSEC Process can apply to any plan, operation, program, project, or activity. It provides a framework for the systematic analyses needed to identify and protect critical information. The process is continuous. It considers the changing nature of critical information and the implementation of threat assessments.

(1) Identify of Critical Information List (CIL). Critical information is needed by adversaries to effectively plan an act to degrade the operational effectiveness of the command. The development of CIL is part of the OPSEC process.

(2) Analysis of Threats. Once adversary collection efforts are identified the aim is to neutralize or manipulate the threat to our advantage. Detailed information about specific intelligence efforts is available from USAG ATO, DPTMS.

(a) Terrorists (Security Plans, Target Locations)

(b) Spies (Research and Development, Equipment)

(c) Criminals (Identity Theft, Financial Gain)

(d) Insiders (All of the above)

(3) Analysis of Vulnerabilities. Analysis of vulnerabilities identifies tentative OPSEC measures required to maintain essential secrecy. The most desirable OPSEC measures combine the highest protection with the least effect on USAG West Point operational effectiveness.

(4) Assessment of Risk. Because the implementation of OPSEC measures usually presents a risk to operational, logistical, or procedural effectiveness, an analysis must be made prior to the decision to implement measures.

(5) Application of Required OPSEC Measures. The application is to identify possible OPSEC measures to mitigate vulnerabilities. The most desirable measures provide needed protection at the least cost to operational efficiency.

(6) USAG West Point personnel should not let everyone know the access procedures used to get on an installation. All personnel should remain vigilant and report any suspicious activity to Law Enforcement personnel and their supervisors.

6. Limits on Secrecy. Care should be taken in determining the required degree of secrecy for undertakings. Too much secrecy has often harmed effectiveness; too little secrecy has resulted in failure. USAG West Point operates in an interagency environment which demands we share information with our partners. Our personnel must be trained to understand how the need to share information with our partners must be balanced against the possible disclosure of that information once it leaves the command. Broad factors to consider include:

a. Adversaries must have some knowledge of friendly capabilities and intentions so they can perceive threats to their operations.

b. The public must know something about military capabilities to foster recruitment of personnel, gain internal political support, ensure understanding of defense budgeting requests, and support defense alliances.

c. Planners must thoroughly understand missions in order to realize and optimize coordination and effectiveness of undertakings.

7. Threat:

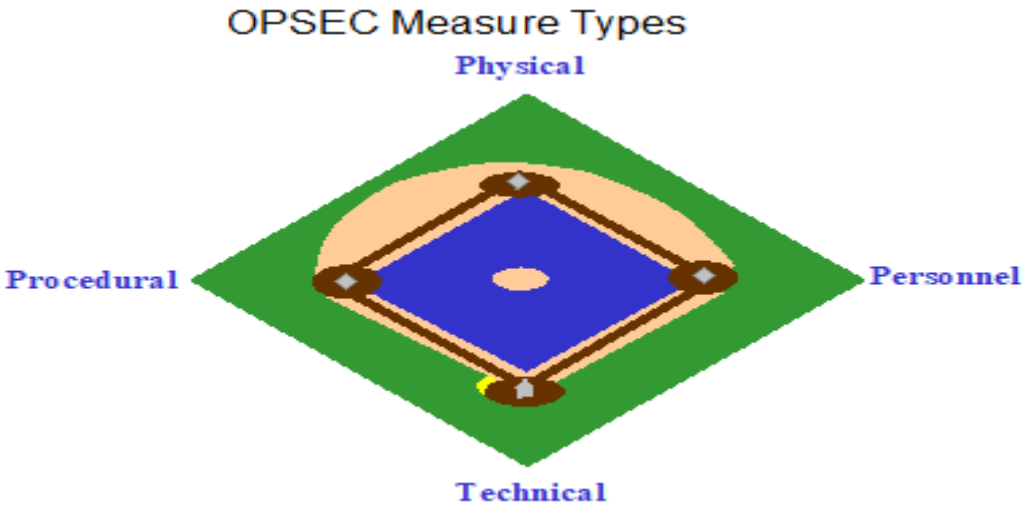
a. USAG West Point offers a lucrative target for hostile intelligence organizations attempting to collect sensitive defense information.

b. There are currently no active National Terrorism Advisory System (NTAS) Alerts. The Defense Intelligence Agency assessment of threat to DOD in CONUS is "Significant."

c. The threat to West Point and its tenant organizations varies depending upon location and unit activity. All tenant organizations must review local threat assessments to determine their threat level. OPMs/Coordinators shall engage interagency partners to coordinate OPSEC requirements, socialize DoD support capabilities, integrate OPSEC into interagency exercises, and enhance engagement with both supported and supporting mission partners.

8. Operations Security Measures.

a. OPSEC measures are in place to protect identified critical information. A good way to evaluate an OPSEC measure is to start by considering its primary intended purpose and then consider any additional functions it performs. Possible OPSEC measures are as varied as the specific vulnerabilities they address. See below diagram.



b. The USAG West Point Garrison Commander has selected the Operations Security measures identified below for implementation as part of USAG West Point ongoing missions and planning for future operations. These OPSEC measures will be monitored by the USAG West Point OPSEC Officers and coordinators. The process is continuous and will consider the changing nature of critical information, and the threats and vulnerabilities of all USAG West Point operations.

(1) Avoid open posting of operation schedules which could reveal when specific events will occur.

(2) Control the issuance of orders for the movement of organizations, programs, or key personnel.

(3) Control trash and housekeeping functions to conceal sensitive missions.

(4) During periods of increased operational activity, adhere to a normal leave policy and working hours to the maximum extent it is possible to preserve the outward impression of normalcy.

(5) Screen discussions or releases to the media with Public Affairs personnel.

(6) Be prepared to implement a "clean desk" policy in the event of visitors.

(7) Limit reading file distribution to personnel with need to know.

8. Contract and Subcontract Requirement:

a. USAG West Point CORs/contractors will use OPSEC measures to protect the organization’s critical information. USAG West Point OPSEC Manager will be responsible for determining OPSEC requirements when the contract involves sensitive but unclassified information.

b. The West Point OPM will identify any OPSEC contractual requirements.

c. It is the responsibility of the OPM, Officers and Coordinators of the USAG West Point to determine what OPSEC measures are essential to protect classified or sensitive information for specific contracts.

d. OPSEC reviews must be included in contracts and subcontracts prior to awarding and funding contracts.

9. Operations Security Review Process/Requirements.

a. OPSEC review is an evaluation of the OPSEC posture of an official document to ensure protection of sensitive or critical information. Official documents may consist of memorandums, letters, messages, briefings, contracts, news releases, technical documents, proposals, plans, orders, response to Freedom of Information Act (FOIA) requests, Privacy Act requests, and other documents.

b. The USAG West Point ATO has 21 days from receipt of contract requirements to complete an OPSEC review and return a signed AT/OPSEC cover sheet.

10. OPSEC Assessment. An annual OPSEC Assessment will be conducted from the period 1 October to 30 September of each fiscal year. The Command OPM and Officers will ensure the assessment IAW regulatory guidance.

11. Survey Requirements. OPSEC Surveys are conducted IAW DoD 5205.02 and AR 530-1, Operations Security. Surveys must be conducted every three years or as requested by the Commander or higher headquarters.

12. Operations Security Level I Education and Awareness Training. All USAG West Point service members, DOD Civilians and contractor personnel will maintain annual OPSEC certification. They will complete OPSEC Level I Awareness training that is composed of both initial and continual awareness training.

13. The United States Army Garrison AT/FP Office is available to assist and support the execution of the above listed measures. Point of contact is Mr. Luke Pagan, DPTMS ATO, at x8859.

STUEWE.DANIEL.R.1074634075
Digitally signed by STUEWE.DANIEL.R.1074634075
Date: 2026.05.12 12:24:56 -04'00'

DANIEL R. STUEWE
COL, IN
Commanding