DEPARTMENT OF THE ARMY
INSTALLATION MANAGEMENT COMMAND
HEADQUARTERS, UNITED STATES ARMY GARRISON WEST POINT
681 HARDEE PLACE
WEST POINT, NY 10996-1554

REPLY TO
ATTENTION OF:

IMML-ZA

11 July 2016

U.S. ARMY GARRISON WEST POINT POLICY #55

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 the 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 City 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 in order 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) will:

(1) Publish a USAG 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 USAG West Point.

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

(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 contract 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 902nd MI and 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. USAG West Point OPSEC Working Group (OWG) will (See Annex D of this Plan):

(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 USAG 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-FH policies and procedures.

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

e. USAG 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 and.

(6) Establish and chair OWG, semiannually.

(7) Ensure OPSEC Officers attend the USAG 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 contract and subcontract documents such as a Request for Proposal (RFP) or Statements of Work (SOW). (For example: Offsite ceremonies, operations, training events, etc)

(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. 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 also inform the chain of command.

1. 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 and vulnerability assessments throughout the operation. It uses the following (5) Five step process:

(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. (For example: Arming of Installation Security Guards; Installation Access control plan or also see Annex C of this Plan.)

(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 West Point Director, DPTMS. (For example: Who is asking about the procedures to get on an installation? What could the people asking for this information do with it? Who are the threats and what are they looking for?) (Also see Annex B of this Plan.)

(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. (For example: Do the Installation guards check everybody or do they just check certain individuals? How many guards are on the gates, and are

they letting all contractors on the installation after checking one person's ID?) (Also see Annex D of this Plan.)

(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. (For example: Are you making a mistake by telling someone else the procedures being used to protect the workforce? Are you making it easy for someone else to cause damage to the Senior Commander Installations by revealing what you know?)

(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. (For example:

(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.)

5. 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.

6. Threat (See Annex B of this OPSEC Plan):

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."

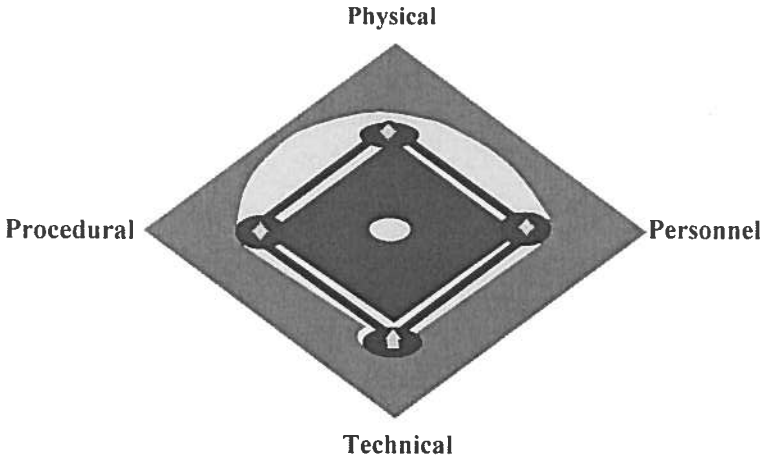
c. The threat to USAG West Point and its tenant organizations varies depending upon location and unit activity. All tenant organizations must review local threat assessments to determine their threat level.

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.

7. 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.

OPSEC Measure Types



Example 1: Access control devices are physical security devices, but they rely on personal security procedures to dictate who should be allowed entry and who should be denied. Access control devices also rely on employee compliance with procedures to pass through such devices and to identify themselves by badge, ID number or biometric measurements.

Example 2: A National Special Security Event is scheduled to be held in Arlington National Cemetery (ANC). An adversary can gain vital information through the media coverage as well as visitor access to ANC and potentially access to the event itself.

b. The USAG West Point Commander has selected the OPSEC 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 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.

c. Readiness.

(1) Safeguard reports on USAG West Point personnel to include attendance at conferences, meetings and/or DOD schools.

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

d. Travel.

(1) Military personnel will travel in Civilian clothes whenever possible. Do not carry briefcases, or bags which identify you as a member of the command.

(2) Use a passport in lieu of military orders whenever possible.

(3) Do not discuss assignment, duties, or reason for travel unless absolutely necessary (e.g., with security, customs, or immigration personnel).

(4) Ensure all military, Civilian, contractor personnel (based upon contract provisions) and Family members traveling on official government orders, receive travel briefings prior to departure for OCONUS destinations. The travel briefing database will be maintained by the Antiterrorism Officer.

(5) Provide protection of travel itineraries for High Risk Personnel/Senior Government Officials (HRP/SGO).

e. Security Awareness Program.

(1) The USAG West Point security education program must generate knowledge and awareness.

(2) Timely coordination with the Command Security Office on security matters will aid in early detection of problem areas and provide improved and expanded support to all
USAG West Point missions. This will permit OPSEC principles, in general, to be given higher visibility and emphasis.

(3) OPSEC and Information Assurance (IA) work together to protect information through policies that achieve acceptable levels of IA in the engineering, implementation, operation, and maintenance of information systems. Official DoD telecommunication systems, including telephones and computer networks, are subject to monitoring at all times for security purposes.

(4) OPSEC guidance and directives will be distributed throughout USAG West Point. These and other informational pamphlets, posters, and announcements provide an educational background and specific guidance of the program.

f. OPSEC Measures. Adherence to the following OPSEC measures is required in order to reduce OPSEC vulnerabilities:

(1) USAG West Point personnel are encouraged to use the STE in the encrypted mode whenever possible, particularly when discussing any technical information.

(2) USAG West Point personnel will not attempt to "talk around" classified information by using code words, catch phrases, or other double-talk.

(3) USAG West Point COMSEC personnel will provide COMSEC briefings and written operating instructions for use of STE phones and monitor the overall COMSEC program.

(4) USAG, F. Hamilton personnel will complete OPSEC awareness training in conjunction with Threat Awareness and Reporting Program (TARP) training, annually.

(5) Enforce a clean desk policy in highly sensitive areas.

(6) Do not take personal cameras, cell phones, pagers, computers, walkmans, radios, CD players, and recording equipment into USAG West Point facilities handling Classified and SCI material.

(7) Protect White boards from casual observation and clear them at the close of business. Charts, graphs, models, equipment parts, etc., must be given the required level of protection to prevent theft and/or unauthorized disclosure.

(8) Visitor reception areas, badges, registration, and escorts, will be used as control measures. Identification badges will be strictly controlled and required for access to sensitive areas. Duplicating a badge is prohibited and holders must certify loss or theft.

(9) Conference rooms and briefing areas will be sanitized prior to sensitive meetings and required precautions exercised, both during and after their use. It is the responsibility of the hosting agency to coordinate these requirements with the Command Security Office and to ensure accomplishment.

(10) Each staff agency and subordinate command will be responsible for identifying specific CIL associated with its missions and the countermeasures necessary for the protection of CIL.

(11) Suspicious vehicles parked or persons loitering near buildings containing ADP facilities or other sensitive electronic processing equipment will be immediately reported to the security manager.

(12) Custodial and maintenance personnel will be escorted in work areas. These areas will be periodically inspected to ensure adherence to contract requirements.

g. Information Assurance (IA)/Cyber Security. IA/Cyber security is critical to the USAG West Point mission success and therefore must be part of your risk management processes. It is essential in assisting with identifying vulnerabilities and taking the necessary steps to conduct daily operations. It is imperative that individuals take

responsibility for identifying potential attacks to their computer and taking the appropriate actions as outlined in annual required IA/Cyber training tracked by the Army Training and Certification Tracking System (ATCTS) at https://atc.us.army.mil https://iatraining.us.army.mil. All users will immediately report network or cyber security incidents to the USAG West Point Installation Operations Center at (718) 630-4271/4296.

Shipment of Sensitive Materials. When shipping sensitive material, USAG West Point personnel will consider the security of the shipment method and review package

h. label markings for sensitive information. Not only are shipments of sensitive material subject to interception, labels placed on packaging can sometimes reveal information regarding the nature of the package contents and its recipients.

i. Public Release.

(1) All news releases will be reviewed by Public Affairs, and will include a documented OPSEC review.

(2) Safeguarded information will not be discussed, shown, or made available to unauthorized individuals.

(3) All DoD personnel must be aware of and support the DoD and Army's OPSEC program.

j. Website OPSEC Reviews. (See Annex H of this OPSEC Plan.)

(1) Commanders will integrate OPSEC reviews of their web sites into their overall OPSEC program and include it in their annual OPSEC Report to the PM/PD.

(2) The OPSEC officer will work with the PAO and Web Master to ensure that Website owners do the following:

(a) Verify that there is a valid need for the distribution/disclosure of the information being posted.

(b) Apply the OPSEC review process IAW DoD 5205.02 and AR 530-1, when clearing information for public distribution.

(c) Protect information according to its sensitivity, and ensure reviewing officials and SharePoint Subject Matter Expert (SME) have received required training in security and release requirements IAW DoD and Army web policies.

(d) Unit commanders, PAOs and SharePoint Subject Matter Expert (SME) should use DoD and Army OPSEC checklists to review content on their publicly accessible websites. (See Annex of this OPSEC Plan.)

k. For Official Use Only (FOUO).

(1) FOUO designation applies to unclassified information, identified by Security Classification Guide (SCG) that is eligible for exemption from mandatory public disclosure under the Freedom of Information Act.

(2) FOUO information includes commercial or financial information generated by or for the Government with the understanding that it is privileged or confidential (e.g. bids, contracts, proposals, trade secrets, inventions, discoveries, proprietary data, or data on contract performance, income, profits, losses, expenditures, etc.).

(3) When instructed by the USAG West Point Commander, material shall be marked FOUO. This category of information is excluded from public release; however, information is not excluded or marked FOUO merely because it is OPSEC sensitive.

(4) To qualify as FOUO information, it must fall under one or more of the exemption categories specified IAW Department of Defense and Army Freedom of Information Act Programs.

8. Contract and Subcontract Requirement(Also refer to Annex H of this Plan):

(1) USAG West Point 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.

(2) The USAG West Point DRM/G8 will identify any OPSEC contractual requirements.

(3) 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.

(4) It is also the responsibility of the OPM, Officers and Coordinators of the USAG West Point to identify those OPSEC measures in their requirements documents and ensure DRM/G8 identifies them in the resulting solicitations and contracts.

(5) OPSEC reviews must be included in contracts and subcontracts prior to awarding and funding contracts.

9. Operations Security Review Process/Requirements.

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. (For example: A cover sheet

a. signed by the OPSEC reviewer, documented, tracked and maintained for future reference.)

b. Procedures.

(1) The OPSEC review may be either directed or requested. A request for an OPSEC review may be initiated by any individual, to the OPM or the OPSEC Officer/Coordinator. Websites should be reviewed quarterly for content IAW AR 25-2.

(2) All news releases will be reviewed by PAO Coordinator and/or Command OPM to include an OPSEC review.

(3) When corrective action is deemed required, to include a classification review, the OPM or Officer will document this in writing to the required official for immediate action.

(4) Technical papers and reports must contain a distribution statement.

(5) OPSEC reviews must be included in contracts and subcontracts prior to awarding and funding contracts.

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. The OPSEC training will also be offered to USAG West Point employee Family members. The OPSEC training can also be found on-line at http://cdsetrain.dtic.mil/opsec/index.htm.

13. The point of contact for this information is Mr. Luke Pagan, Directorate of Plans, Training, Mobilization and Security, at (845) 938-8859.

ANDREW S. HANSON
Colonel, SF
Commanding

10 Encls
1. Annex A
2. Annex B
3. Annex C
4. Annex D
5. Annex E
6. Annex F
7. Annex G
8. Annex H
9. Annex I
10. Annex J

Annex A to USAG West Point OPSEC PLAN
References

a. National Security Decision Directive 298 Chairman (NSDD 298), dated 22 January 1988.

b. Chairman, Joint Chiefs of Staff Instruction 3213.01D, Joint Operations Security, dated 7 May 2012.

c. Joint Pub 3-13.3, Operations Security, dated 4 January 2012.

d. Department of Defense Directive 5205.02, Operations Security (OPSEC) Program, dated 20 June 2012.

e. AR 530-1, Operations Security, dated 17 April 2007 (In revision).

f. AR 25-55, Department of the Army Freedom of Information Act Program, dated 1 November 1997.

g. AR 1-201, Army Inspection Program, dated 4 April 2004.

h. AR 380-5, Department of the Army (DA) Information Security Program, dated 29 September 2000.

i. AR 380-10, Technology Transfer, Disclosure of Information and Contacts with Foreign Representatives, dated 22 June 2005.

j. AR 381-12, Threat Awareness and Reporting Program (TARP), dated 10 October 2010.

k. AR 25-1, Army Knowledge Management and Information Technology, dated 25 June 2013.

l. AR 25-2, Information Assurance, dated 23 March 2009.

m. AR 360-1, Army Public Affairs Program, dated 25 May 2011.

n. DOD Directive 5205.7, Special Access Program, dated 1 July 2010.

o. AR 380-381, Special Access Programs, dated 21 April 2004.

p. DOD Instruction 5220.22, National Industrial Security Program, dated 15 March 2013.

q. FM 3-13, Inform and Influence Activities, dated 25 January 2013.

r. FM 5-0, Army Planning and Orders Production, dated 20 January 2005.

s. FM 6-0, Mission Command: Command and Control of Army Forces, dated 11 August 2003.

t. FM 90-2, Tactical Cover and Deception, dated 3 October 1998.

u. Joint Pub 1-02, DOD Dictionary of Military and Associated Terms, dated 8 November 2010 (As Amended Through 15 June 2013).

v. Joint Pub 3-0, Doctrine for Joint Operations, dated 10 September 2001.

w. Joint Pub 3-13, Information Operations, dated 13 February 2006.

x. Joint Pub 3-13.4, Military Deception, dated 13 July 2006.

y. Joint Pub 5-03.1, Joint Operation Planning and Execution System, Volume II, Planning and Execution Formats and Guidance, dated 4 August 1993.

Annex B to USAG West Point OPSEC PLAN
Intelligence Threats

B-1. Listed below are some examples of specific types of threats within each of the major categories. The Multidiscipline Counterintelligence Threat for USAG West Point JOA is located in a separate Plan.

a. Foreign Intelligence Service Threat.

(1) Human Intelligence (HUMINT) (e.g., recruitment, blackmail, surreptitious entry, phone taps, bugs, unauthorized computer access, etc.)

(2) Signals Intelligence (SIGINT) (e.g., intercept/exploit communications, computer data, TEMPEST, etc.)

(3) Imagery Intelligence (IMINT) (e.g., overhead imaging, hand held photography, etc.)

(4) Measurement and Signature Intelligence (MASINT) (e.g. radar intelligence, infrared intelligence and nuclear intelligence.)

(5) Open Source Intelligence (OSINT) (e.g., Websites, public releases, newspapers, etc).

b. Terrorist Threat.

(1) Assassination.

(2) Bombing.

(3) Kidnapping.

(4) Radiological, Biological, Chemical, Nuclear attacks.

(5) Stand-off weapons attacks/Raids.

c. Insider Threat.

(1) Malicious acts by disgruntled personnel (violence, sabotage).

(2) Espionage/theft of classified material for adversary.

(3) Unauthorized disclosure of classified material.

(4) Theft of property.

(5) Inadvertent loss of classified material.

d. Criminal Threat (Outsider):

(1) Violent acts against people.

(2) Theft/destruction of property.

(3) Mob Violence.

(4) Hacking/Cracking of Computer Systems.

e. Environmental Threat:

(1) Fire.

(2) Storm.

(3) Pollution.

(4) Earthquake.

(5) Flood.

f. Military Threat:

(1) Nuclear/Radiological/Biological/Chemical.

(2) Conventional/Unconventional Warfare.

(3) Information Warfare.

g. Cyber Threat:

(1) Government Computer Networks.

(2) Cyber Warfare.

(3) Critical Sensitive Information.

(4) NIPRNET.

(5) Open Source (Adversary receives over 90% of resources from Open Source).

Annex C to USAG West Point OPSEC PLAN

Critical Information List (CIL)

C-1. This Plan identifies USAG West Point CIL that must be protected from adversarial exploitation.

a. The CIL includes specific facts about friendly intentions, capabilities, and activities needed by adversaries to plan and act effectively against friendly mission accomplishment. Critical information is susceptible to collection by adversaries through indicators (friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information), and vulnerabilities (conditions in which friendly actions provide OPSEC indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decision making).

b. USAG West Point CIL:

(1) Information pertaining to access control, physical security, and protection of installations and critical assets (e.g., personnel, facilities, equipment, or information). (OPR: PM/PD)

(2) Current and projected operational status (including capabilities and readiness) of assigned forces and command and control (C2) systems. (OPR: G3, OCR: G6)

(3) Information regarding deployment/redeployment of JFHQ-NCR /USAMDW personnel and assets to support real-world missions (i.e. overseas contingency operations). (OPR: G3)

(4) Location/disposition of forces during events or incident response, including all DoD and interagency response forces. (OPR: G36, OCR: G35)

(5) Posture or preparation of Base Support Installations (BSI) in support of Joint Reception, Staging, Onward Movement & Integration (JRSOI) operations. (OPR: G3, OCR: G1/G4)

(6) Operational requirements, capabilities, or shortfalls pertaining to preparation and execution of USAG West Point COOP/COG operations. (OPR: G3, OCR: PM/PD)

C-2. Other critical information to consider during operations is:

a. Budget. Prioritization, preparation and distribution of annual budget; Increases/decreases to budget Costs of future force bed down/mission changes; Emergency requisition of funds that discloses details of contingency/wartime ops.

b. Intelligence/Planning. Targets and Purpose of Effort; US/Coalition Objectives; Rules of Engagement; Plan Schedules/Sequences of Events; Intelligence Sharing Relationships; Intelligence Gaps/Unknowns; Planning Procedures ; Photos revealing operational capabilities of critical systems.

c. Logistics/Information Systems. System Passwords with Usernames; IP Addresses with Functions; Equipment Acquisition; Equipment Status/Location; Maintenance Schedule; System Architecture/Configuration; Critical C2/C4I Nodes; Power and HVAC Nodes; Relocation Plans/Procedures; Connectivity Limitations; Communication Outages.

d. Operations. Limitations/Weaknesses/Shortfalls; FP/Anti-Terrorism Measures; Recall Procedures; battle Rhythm; Operational Briefings; Results of Exercises, Ops, Training; Codenames and Operational Details; Operational Targets and Objectives; Asset Regeneration; Patterns of Mission Performance; Required Equip, Hardware, Software; Deployment Capabilities/Limitations; Emergency Action Procedures; TTPs of any Unit Asset; FOUO markings on all C-IED products IAW ALARACT 271-2010.

e. Personnel/Security. Personnel Manning Strength; Access/Authentication Procedures; Security Alarm Limitations/Outages; Status of Readiness and Training; Security Clearance Information; Distinguished Visitor/High Risk Personnel/Senior Government Official Information/travel/itinerary; MEVAs/High Risk Targets (HRTs).

f. Plans. Changes in National Security Special Event (NSSE) mission/tasking; Specific information of deployment location/equipment; Security classification of a classified operation, program, or project; Intent to mobilize before public announcement; Infrastructure reports; COOP Planning (evacuation routes/procedures and rally points).

Annex D to USAG West Point OPSEC PLAN

OPSEC Working Groups (OWG)

D-1. General. An OWG, through the ATWG, will be established to ensure compliance with OPSEC regulatory guidelines.

a. The Intent is to assist the USAG West Point Commander, Installation Commanders and Major Subordinate Commands involved in the implementation of OPSEC programs and to ensure OPSEC measures are planned, coordinated, and implemented to preserve essential secrecy with every phase of each sensitive operation, exercise, or event.

b. The OWG assists the commander and the OPM/Officer in ensuring continuity of effort in developing, implementing, and monitoring his/her organization's OPSEC program.

c. The working group formulates and implements approved OPSEC policies and procedures for the USAG West Point.

d. To maximize critical resources, OPSEC, Security, Information Operations, Law Enforcement (LE), Intelligence (Intel) Physical Security (PS) and Antiterrorism/Force Protection (AT/FP) personnel will be permanent members of the working group.

D-2. Purpose. This annex establishes the USAG West Point OWG Charter. The OWG has authority to determine the priorities for OPSEC considerations and to direct the implementation of OPSEC measures.

D-3. References. CJCS Instruction 3213.01D, Joint Operations Security, DoD Directive 5205.2, DoD OPSEC Program, AR 530-1, Operations Security (OPSEC), AR 25-55, Department of Army Freedom of Information Act Program, FM 101-5, Staff Organization and Operations, FM 3-13, Inform and Influence Activities, DA Pamphlet 190-51, Risk Analysis foe Army Property, DoD Directive 2100.12, AT/FP Program, AR 525-13, Antiterrorism, and CSA/VCSA guidance.

D-4. Policy. OWG members and alternates will possess required security clearances.

D-5. Objectives. The objectives of the OWG are to:

a. Review and coordinate OPSEC program directives and initiatives, and review OPSEC reports to develop trends, indicators, patterns, and profiles of intelligence value.

b. Devise methods for improving the OPSEC posture of USAG West Point and its' subordinates.

c. Develop OPSEC measures and deception tactics.

d. Determine the impact of open source publications (such as newspaper articles, press releases, and so forth) on USAG West Point programs, projects, and missions.

e. Provide command emphasis for OPSEC missions.

f. Review, coordinate, and recommend OPSEC policy, programs, and objectives.

g. Conduct reviews of initiatives for improving the USAG West Point OPSEC posture, to include review of the USAG West Point annual OPSEC report prior to transmittal to HQDA.

h. Recommend subjects, dates, and times for OPSEC assessments and surveys.

i. Prioritize requests for external intelligence and security support.

j. Direct the development and implementation of OPSEC measures.

D-6. Responsibilities:

a. Chairperson. The chairperson of the OWG will:

(1) Determine the composition of the OPSEC Working Group.

(2) Develop, recommend, and coordinate agenda items for the OWG chairperson's approval.

(3) Report OWG actions and recommendations to the commander.

(4) Schedule and preside over OWG meetings.

(5) Request briefings on specific matters of OPSEC concern from the required staff section or activity.

(6) Ensure a copy of the OWG meeting minutes is provided to the commander.

b. Membership. Regular members of the USAG West Point OWG will be:

(1) USAG West Point commander or designated representative.

(2) USAG West Point OPM and/or Assistant, Coordinator, and the OPSEC Officer from each installation and Major Subordinate Command.

(3) Representative from each USAG West Point Directorate and Staff Section that normally attend operational working groups.

c. Additional Representatives. Other personnel may attend at the invitation of the primary representative if advance notice is provided to the USAG West Point OPM/Officer. If others are requested to attend they must submit security clearance to the USAG West Point Security Officer for verification.

Annex E to USAG West Point OPSEC PLAN

Vulnerability Assessments (VA):

E-1. Vulnerabilities are friendly actions that provide indicators that may be obtained and accurately evaluated by an adversary to provide a basis for effective adversary decision making. Vulnerabilities consist of stereotyped actions that habitually occur (patterns), and unique detectable characteristics that identify the type of activity or intention (signatures). OPSEC vulnerability exists when these conditions are met:

a. The adversary can collect an indicator of critical information,

b. Correctly analyze the information,

c. Make a decision,

d. And take timely action to adversely influence, degrade or prevent friendly operations.

E-2. The following vulnerabilities, if detected by an adversary, could be used to the disadvantage of USAG West Point missions and OPSEC measures must be established to protect these potential OPSEC vulnerabilities:

a. Information Security Vulnerabilities.

(1) Failure of USAG West Point personnel to ensure that classified or sensitive unclassified information is furnished or disclosed only to authorized personnel.

(2) Failure to provide a security review for classified information resulting in inadvertent disclosure of classified information.

(3) Employment of un-cleared personnel to duties that may provide the opportunity for access to classified information.

(4) Failure to follow security classification guidelines for proper classification of data.

(5) Failure of planners to determine the threat/risk prior to beginning USAG WEST POINT missions.

b. Operations Security Vulnerabilities.

(1) Open sources whereby documents are published and distributed without OPSEC reviews or limited distribution statements as applicable.

(2) Improper disposal of sensitive, unclassified information.

(3) Lack of awareness as to the adversary collection threat to USAG West Point operations causing personnel to become careless in their day-to-day OPSEC and other security responsibilities.

(4) Failure on the part of USAG West Point personnel to adequately review security requirements during planning and exercises.

(5) Military blogs which provide information that enhances the enemy's targeting process.

c. Physical Security Vulnerabilities:

(1) Failure to maintain or enforce access controls for designated controlled or restricted areas.

(2) Failure to maintain strict key and lock accountability for facilities that contain USAG West Point information.

(3) Failure to follow procedures for critical test and maintenance of intrusion detection systems.

(4) Failure to follow established procedures in the control and movement of vehicles entering or leaving restricted areas.

d. Computer Network Defense Vulnerabilities:

(1) Human error that results in the accidental destruction, disclosure, or modification of sensitive and classified computer-based information.

(2) The processing of classified or sensitive data on a CND system which has not been approved or accredited for such information through the intentional disregard of policy.

(3) Computer transmissions that could be intercepted causing an unauthorized disclosure of sensitive data.

(4) Lack of adequate encryption capabilities.

(5) Insufficient training in CND security features and requirements for CND system administrators.

(6) Lack of anti-virus and patches on CND systems.

e. Anti-Terrorism /Force Protection (AT/FP) Vulnerabilities:

(1) Current threat and Force Protection Condition level (FPCON).

(2) Type/number/mix of personnel and security equipment available or in use at this location, and other USAG West Point AOR. What are their capabilities?

(3) Personal Security Detail (PSD) team schedule and requirements for mission execution.

(4) Physical security measures implemented at all USAG West Point AOR locations.

(5) Location of critical facilities and nodes to include Air Point-of-De/Embarkations (APOD/APOE), Sea Port of De/Embarkations (SPOD/SPOE), and Mission Essential Vulnerable Areas (MEVA).

Annex F to USAG West Point OPSEC PLAN

OPSEC Training:

F-1. General:

a. For the USAG West Point OPSEC program to be effective, all assigned soldiers, Civilians, and DoD contractors, must understand the concept of OPSEC. They must also apply the knowledge and awareness in the performance of their day-to-day activities.

b. In order for the USAG West Point OPSEC training program to comply with all DOD and HQDA policies and regulations it must be action and job-oriented over time. The content of material presented during all OPSEC training will be selected to answer four primary questions the audience is likely to ask.

(1) What is OPSEC?

(2) Why is OPSEC important to me?

(3) Why is OPSEC important to my organization?

(4) How can I contribute to the OPSEC program?

F-2. USAG West Point OPSEC Training Programs:

a. Initial OPSEC Awareness Training. The OPSEC Manager, Officer and/or Coordinator will provide all newly assigned personnel OPSEC Awareness training within the first 30 days of their arrival in USAG West Point. This training will focus on the following areas:

(1) Understanding USAG West Point CIL.

(2) The local, multidiscipline adversary intelligence threat.

(3) How adversaries aggressively seek information on U.S. military capabilities, intentions, and plans.

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

(5) Specific guidance on OPSEC measures to protect Critical Information from inadvertent disclosure.

b. Continual OPSEC Awareness Training. The OPSEC Manager, Officer and/or Coordinator will continually provide OPSEC awareness training to the workforce, reemphasizing the importance of sound OPSEC practices.

(1) This training consists of, but is not limited to, periodic OPSEC news releases in local command publications, OPSEC posters in unit areas, OPSEC information bulletins on unit bulletin boards and OPSEC awareness briefings by unit commanders.

(2) At a minimum, all DOD personnel must receive an annual OPSEC awareness training briefing provided by the USAG West Point OPSEC Manager, Officer and/or Coordinator. This training must be updated with current information and tailored for the unit's specific mission and critical information.

(3) OPSEC training will be provided to deploying and redeploying units.

(4) OPSEC officer will produce and make available OPSEC training for Family Readiness Groups (FRGs) at meetings, commander's call, and town meetings.

(5) The OPSEC training can also be found on-line at: (http://cdsetrain.dtic.mil/opsec/index.htm).

c. OPSEC Officer Training. Commanders will provide OPSEC officers and other staff personnel with training opportunities that will teach the skills necessary to prepare OPSEC estimates, to prepare OPSEC planning guidance, to plan OSPEC measures, to write OPSEC plans and annexes, and to supervise the execution of OPSEC measures. The following training is required:

(1) Program Manager is required to attain Level II certification and strongly recommended to attain Level III certification.

(2) OPSEC Officer is required to attain Level II certification and is encouraged to attend Level III certification based on recommendation from the chain of command and OPM.

(3) OPSEC Coordinator is required at a minimum to complete OPSE 1301 or equivalent. If executing duties as described in paragraphs H-3 or H-4, these individuals are now performing the duties of an OPSEC Officer and; will attend OPSEC Level II certification.

(4) Level II certification must be attained within 90 days of appointment.

Annex G to USAG West Point OPSEC PLAN

OPSEC Program Matrix

REQUIREMENTS	CDRs	OPSEC Officer/ Manager	STAFF	PAO	SharePoint SME	All Personnel	REMARKS
Establish an active and documented OPSEC program.	X	X	X	X	X		DoD missions, agencies, installations, and staff organizations will have functional, active, and documented OPSEC programs. Paragraphs 2-3. a. (3) and 3-1.
Appoint an OPSEC Officer and/or Coordinator in writing.	X		X	X	X		Paragraphs 2-3. a. (1) and 3-2. A.
Develop, organize and administer OPSEC program at JFHQ-NCR /USAMDW, Installations, /Garrisons, Subordinate Commands and their battalions.		X	X	X	X		Paragraph 3-2. a. (1).
Ensures that appointed OPSEC Officer receives required training.	X	X	X	X	X		Paragraphs 2-3. a. (2), 3-2 (4) & 4-2. b.
Provides guidance and oversight to multiple subordinate OPSEC programs of various units, missions, and organizations.		X	X	X	X		Paragraph 3-2. a. (1).

Develop OPSEC SOP.		X	X	X	X		Documents the unit critical information and OPSEC measures to protect it. Paragraph 3-2.
If assigned intelligence and counterintelligence (CI) capabilities, provide intelligence and CI support to the command's OPSEC program.	X	X					Paragraph 2-3. a. (4).
Write OPSEC, Plans, SOPs, Annexes & OPORDs.		X	X	X	X		Paragraphs 2-3. a. (3), 3-2 and 3-2. c.
Develop and propose the CIL to the Commander for approval.		X	X	X	X		Paragraph 2-3. a. (5).
Approve the unit, activity, or installation CIL.	X						Paragraph 2-3. a. (5).
Conducts initial operations security Awareness Training.		X	X	X	X		All newly assigned personnel within the first 30 days of arrival in the organization (this includes accessions and initial entry programs) must receive initial training. Paragraph 4-2. a. (1).

Conducts continuous operation security Awareness Training.		X	X	X	X		This training consists of, but is not limited to, periodic OPSEC news releases in local command publications, OPSEC posters in unit areas, OPSEC information bulletins on unit bulletin boards and OPSEC awareness briefings by unit commanders at commander's calls. Paragraph 4-2 a. (2) (a) (b).
Provide OPSEC training to deploying and redeploying units, to include Family readiness groups (FRGs).		X	X	X	X		Paragraph 4-2. a (2) (c).
Receive annual OPSEC awareness training.	X	X	X	X	X	X	At a minimum, all DoD personnel mus receive an annual OPSEC awareness training briefing provided by the unit or organization's OPSEC Officer. Paragraph 4-2 a. (2) (b).
Conduct OPSEC Reviews.		X	X	X	X		Paragraph 5-1.
Conduct OPSEC Web site reviews.		X		X	X		The OPSEC Web site review is the responsibility of the SharePoint Subject Matter Expert (SME), in coordination with the OPSEC officer, PAO, and other required designees (security and intelligence, command counsel, and so forth.). Paragraphs 2-2. c. & 5-2. d. (2).

Compare the identified indicators with the adversary's intelligence collection capabilities.		X	X				In coordination with the intelligence staff and all other staff elements, examine each part of the activity/operation to find actions or information that will provide indicators in each area (personnel, logistics communications, movement missions aviation, and so forth.). Paragraph B-3. b. (1).
Conduct analysis of vulnerabilities.		X	X				Analyze what critical information friendly forces are exposing. Paragraph 3-2. b. (1) (c).
Conducts OPSEC assessments.		X	X	X	X		The OPSEC officer conducts OPSEC assessments of subordinate units using the published OPSEC guidance to determine if the unit being assessed is implementing higher headquarters directed and their own OPSEC policies and procedures. Paragraph 5-4.
Determines OPSEC requirements when the contract involves sensitive information.		X	X	X	X		Chapter 6.
Consider OPSEC in all unit missions.	X	X	X	X	X	X	Paragraph 1-8. b.
Decide which, if any, OPSEC measures to recommend for implementation and when to do so.		X					B-5. b.
Approve OPSEC measures.	X						B-6. a.

Implement OPSEC measures.	X	X	X	X	X	X	The OPSEC Officer implements the OPSEC measures and then unit personnel implement the OPSEC measures. B-6.
Evaluate the effectiveness of OPSEC measures during execution.		X	X	X	X	X	

Annex H to USAG West Point OPSEC PLAN

AT/OPSEC Contract Requirements Package

Contract Requirements Package Antiterrorism/Operations Security Review Cover Sheet

Requirements Package Title _____ Date _____

Section I.

Purpose of cover sheet: To document the review of the requirements package requirements performance work statement (PWS), quality assurance surveillance plan and any applicable source selection evaluation criteria for antiterrorism (AT) and other related protection matters to include, but not limited to: AT, operations security (OPSEC), information assurance (IA), physical security, law enforcement, intelligence, foreign disclosure.

Army policy requirement: A signed AT/OPSEC cover sheet is required to be included in all requirements package except for supply contracts under the simplified acquisition level threshold, field ordering officer actions and Government purchase card purchases. Command policy may require this form for supply contracts under the simplified acquisition level threshold.

Mandatory review and signatures: The organizational antiterrorism officer (ATO) must review each requirements package prior to submission to supporting contracting activity to include coordination with other staff review as appropriate per section II below. If the requiring activity does not have an ATO, the first ATO in the chain of command will review the contract for considerations. An OPSEC officer review is also mandatory.

Section II. Standard Contract Language Provision/Contract Clause Text Applicability and/or Additional PWS Language. If standard contract or clause language found on page 2 (Section IV) of this form is sufficient to meet specific contract request requirements, check "yes" in block below and include this language in the PWS. If standard contractual text (provisions or clauses) or clause language does not apply, check "no." If the standard PWS language applies, but is not in of itself sufficient, check "yes" and "PWS" and include both the standard language and additional contract specific language in the PWS. If standard contract al text or clause language is not desired, but there is related contract specific language in the PWS, check "no" and "PWS."

1. AT level 1 training (general)	____YES	___NO	___PWS
2. Access and general protection policy and procedures	____YES	___NO	___PWS
3. AT awareness training for US based contractor personnel traveling overseas	____YES	___NO	___PWS
4. iWATCH training	____YES	___NO	___PWS
5. Access to government information systems	____YES	___NO	___PWS
6. Special OPSEC program requirements	____YES	___NO	___PWS
7. Requirement for OPSEC training	____YES	___NO	___PWS
8. Information assurance/information technology training	____YES	___NO	___PWS

9. Information assurance/information technology certification	____YES	___NO	___PWS
10. Contractor Authorized to Accompany the Force clause	____YES	___NO	___PWS
11. Contract requiring performance or delivery in a foreign country	____YES	___NO	___PWS
12. Handling/Access to Classified Information	____YES	___NO	___PWS
13. Appropriate HSPD-12 Related Access	____YES	___NO	___PWS

Section III. Remarks:

Antiterrorism Review Signature: I am an ATO (Level II Certified) and have reviewed the requirements package and understand my responsibilities in accordance with Army Regulation 525-13, Antiterrorism.

Reviewer

_____

Typed or printed name, rank/civ grade

_____

Signature

Date _____

Phone Number _____

Operations Security Review Signature: I am OPSEC level II certified and have reviewed the requirements package, and it is in compliance with Army Regulation 530-1, Operations Security.

Reviewer

_____

Typed or printed name, rank/civ grade

_____

Signature

Date _____

Phone Number _____

Additional comments:

Section IV. Standard Contract Language/Contract Clause Applicability and/or Additional PWS Language.

1. AT Level I Training. This standard language is for contractor employees with an area of performance within an Army controlled Installation, facility or area. All contractor employees, to include subcontractor employees, requiring access Army installations, facilities and controlled access areas shall complete AT Level I awareness training within XX calendar days after contract start date or effective date of incorporation of this requirement into the contract, whichever is applicable. The contractor shall submit certificates of completion for each affected contractor employee and subcontractor employee, to the COR or to the contracting officer, if a COR is not assigned, within XX calendar days after completion of training by all employees and subcontractor personnel. AT level I awareness training is available at the following website: https://atlevel1.dtic.mil/at.

2. Access and General Protection/Security Policy and Procedures. This standard language is for contractor employees with an area of performance within an Army controlled installation, facility or area. Contractor and all associated sub-contractors employees shall comply with applicable installation, facility and area commander installation/facility access and local security policies and procedures (provided by government representative). The contractor shall also provide all information required for background checks to meet installation access requirements to be accomplished by installation Provost Marshal Office, Director of Emergency Services or Security Office. Contractor workforce must comply with all personal identity verification requirements as directed by DOD, HQDA and/or local policy. In addition to the changes otherwise authorized by the changes clause of this contract, should the Force Protection Condition (FPCON) at any individual facility or installation change, the Government may require changes in contractor security matters or processes.

3. AT Awareness Training for Contractor Personnel Traveling Overseas. This standard language required US based contractor employees and associated sub-contractor employees to make available and to receive government provided area of responsibility (AOR) specific AT awareness training as directed by AR 525-13. Specific AOR training content is directed by the combatant commander with the unit ATO being the local point of contact.

4. iWATCH Training. This standard language is for contractor employees with an area of performance within an Army controlled installation, facility or area. The contractor and all associated sub-contractors shall brief all employees on the local iWATCH program (training standards provided by the requiring activity ATO). This local developed training will be used to inform employees of the types of behavior to watch for and instruct employees to report suspicious activity to the COR. This training shall be completed within XX calendar days of contract award and within YY calendar days o new employees commencing performance with the results reported to the COR NLT XX calendar days after contract award.

5. Contractor Employees Who Require Access to Government Information Systems. All contractor employees with access to a government info system must be registered in the ATCTS (Army Training Certification Tracking System) at commencement of services, and must successfully complete the DOD Information Assurance Awareness prior to access to the IS and then annually thereafter.
6. For Contracts that Require a Formal OPSEC Program. The contractor shall develop an OPSEC Standing Operating Procedure (SOP)/Plan within 90 calendar days of contract award, to be reviewed and approved by the responsible Government OPSEC officer. This plan will include a process to identify critical information, where it is located, who is responsible for it, how to protect it and why it needs to be protected. The contractor shall implement OPSEC measures as ordered by the commander. In addition, the contractor shall have an identified certified Level II OPSEC coordinator per AR 530-1.
7. For Contracts that Require OPSEC Training. Per AR 530-1 Operations Security, the contractor employees must complete Level I OPSEC Awareness training. New employees must be trained within 30 calendar days of their reporting for duty and annually thereafter.

8. For Information assurance (IA)/information technology (IT) training. All contractor employees and associated sub-contractor employees must complete the DoD IA awareness training before issuance of network access and annually thereafter. All contractor employees working IA/IT functions must comply with DoD and Army training requirements in DoDD 8570.01, DoD 8570.01-M and AR 25-2 within six months of appointment to IA/IT functions.

9. For information assurance (IA)/information technology (IT) certification. Per DoD 8570.01-M , DFARS 252.239.7001 and AR 25-2, the contractor employees supporting IA/IT functions shall be appropriately certified upon contract award. The baseline certification as stipulated in DoD 8570.01-M must be completed upon contract award.

10. For Contractors Authorized to Accompany the Force. DFARS Clause 252.225-7040, Contractor Personnel Authorized to Accompany U.S. Armed Forces Deployed Outside the United States. The clause shall be used in solicitations and contracts that authorize contractor personnel to accompany US Armed Forces deployed outside the US in contingency operations; humanitarian or peacekeeping operations; or other military operations or exercises, when designated by the combatant commander. The clause discusses the following AT/OPSEC related topics: required compliance with laws and regulations, pre-deployment requirements, required training (per combatant command guidance), and personnel data required.

11. For Contract Requiring Performance or Delivery in a Foreign Country, DFARS Clause 252.225-7043, Antiterrorism/Force Protection for Defense Contractors Outside the US. The clause shall be used in solicitations and contracts that require performance or delivery in a foreign country. This clause applies to both contingencies and non-contingency support. The key AT requirement is for non-local national contractor personnel to comply with theater clearance requirements and allows the combatant commander to exercise oversight to ensure the contractor's compliance with combatant commander and subordinate task force commander policies and directives.

12. For Contracts That Require Handling or Access to Classified Information. Contractor shall comply with FAR 52.204-2, Security Requirements. This clause involves access to information classified "Confidential," "Secret," or "Top Secret" and requires contractors to comply with (1) The Security Agreement (DD Form 441), including the National Industrial Security Program Operating Manual (DoD 5220.22-M); (2) any revisions to DOD 5220.22-M, notice of which has been furnished to the contractor.

13. Apply Appropriate HSPD-12-Related Access. Contractor shall comply with requirements expressed in HSPD-12. Ensure that non-Federal Government and non-DoD-issued card holders who are given unescorted access to DoD installations to be identity proofed and vetted to determine fitness and eligibility for access. Personnel must be vetted against government authoritative data sources, to include the National Crime Information Center (NCIC) and Terrorist Screening Database (TSDB).

Annex I to USAG West Point OPSEC PLAN

OPSEC Checklist

All Purpose Checklist		Page 1 Of 3 Pages		
Title/Subject/Command/Functional Area Operations Security (OPSEC) Checklist		Date		
No	Items	Yes	No	N/A
	Responsibilities			
1.	Does the organization have a written OPSEC program down to battalion level? (AR 530-1, 2-3. a., 3-1)			
2.	Does the organization have a written OPSEC Plan to protect sensitive and critical information? (AR 530-1, 3-2)			
3.	Has an OPM or OPSEC Officer been appointed in writing. (AR 530-1, paragraph 3-2. a.)			
4.	Are the OPSEC Managers, OPSEC Officers and Coordinators knowledgeable of their duties? (AR 530-1, Appendix H)			
5.	Has the appointed OPSEC officer or OPM attended the HQDA OPSEC Officer/Program Manager certification course conducted by the DoD and Army OPSEC Support Element (OSE)? (AR 530-1, 4-2. b.)			
6.	Has the commander established OPSEC as a command emphasis item and included OPSEC effectiveness as an evaluation objective for all operations, exercises, and missions? (AR 530-1, 2-3. a. (12)			
7.	Has the commander approved the organization's unit or installation CIL? (The OPSEC Officer or Program Manager will develop and propose the CIL to the Commander for approval) (AR 530-1, 2-3. a (5)			
8.	Are all DoD and Army personnel (the total workforce consisting of Soldiers, DA Civilians, and DOD contractors) receiving Initial OPSEC Awareness Training within the first 30 days of arrival in the organization? (AR 530-1, 4-2 a. (1))			

9.	Does each individual know the answers to the following questions: (AR 530-1, 4-2. a. (1) a. What is my unit or organization's critical information? b. What critical information am I personally responsible for protecting? c. How is the threat trying to acquire my critical information? d. What steps am I/are we taking to protect my/our critical information? e. Who is my OPSEC Officer and/or Coordinator?			
10.	Does the OPSEC training program include Continuous OPSEC Awareness Training? (AR 530-1, 4-2. a. (2).			
11.	Does the Commander of USAG West Point submit the Command's Annual OPSEC Report for the fiscal year (FY) to the DoD and Army OPSEC Support Element (OSE)? (AR 530-1, 2-4. d.) SCs, GCs, MSCs and SRUs will send a report to their respective ACOM, ASCC, or DRU. (AR 530-1, Appendix I-1. a).			
	Web Sites			
	Are commanders and supervisors responsible for complying with Federal, DoD, and DA Web site administration policies and implementing content-approval procedures that include OPSEC and PAO reviews before updating or posting information on all Web sites (AR 25-2, 4-20.(11))=.			
	Are commanders conducting annual OPSEC reviews of all organizational Web sites and including these results in their annual OPSEC reports pursuant to AR 530-1 (AR 25-2, 4-20.g.(15).			
	Have all organizational web sites received an OPSEC web site review to ensure no information in accordance with AR 25–2, paragraph 6–4n(4), is contained on any publicly accessible web site. The OPSEC Web site review is the responsibility of the SharePoint Subject Matter Expert (SME), in coordination with the OPSEC officer, PAO, and other required designees (security and intelligence, command counsel, and so forth) (AR 530-1, 5-2. d. (1) & (2).			
	FOIA/Privacy Act/Contracts			
	Are responses to Freedom of information Act (FOIA), or Privacy Act requests receiving OPSEC review? (AR 530-1, 5-1)			
	Is OPSEC incorporated into all classified contracts as well as unclassified contracts that involve sensitive information? (AR 530-1, 2-3.a. (11) also see chap 6–2.)			
	PAO			

	Is OPSEC considered in all public affairs operations? (AR 525-13, Appendix C-4.d (4).			
	Does the staff office or agency providing the information, materials, or records to the PA office for release, accomplish OPSEC reviews? (AR 360-1, 5-4)			
	Internet and Intranet allow the commander to further increase the distribution of print and broadcast mediums to reach a wider audience. Creators and designers of this material will ensure it meets OPSEC requirements (AR 360-1, 5-6 c (4).			
	Commanders and supervisors are responsible for complying with Federal, DOD, and DA Web site administration policies and implementing content-approval procedures that include OPSEC and PAO reviews before updating or posting information on all Web sites (AR 25-2, 4-20.g.(11).			

Annex J to USAG West Point OPSEC PLAN
Glossary of Abbreviations/Terms

ACOM	Army Command. An Army force, designated by the Secretary of the DoD and Army, performing multiple Army Service Title 10 functions (3013b) across multiple disciplines. Command responsibilities are those established by the Secretary.
Adversary	Those individuals, groups, or organizations that must be denied critical information to maintain friendly mission effectiveness. Adversaries may include hostile countries, terrorists and allied intelligence agencies.
AIS	Automated Information System
AAOG	Army Air Operations Group
AR	Army Regulation
ASCC	Army Service Component Command. An Army force, designated by the Secretary of the Army, comprised primarily of operational organizations serving as the Army component of a combatant command or a sub-unified command. If directed by the combatant commander, an ASCC serves as a Joint Forces Land Component Command (JFLCC), or Joint Task Force (JTF).
CIL	Critical Information List
Collection Threat	Collection of information on U.S. Army missions may be conducted by adversaries using various intelligence collection methods. These pieces of information provide an accurate portrayal of the commands overall intentions and/or operations.
C2	Command and Control
C2W	Command and Control Warfare
Communication Security (COMSEC)	Communications Security. This material is controlled and managed under a separate set of security standards and procedures from those that apply to other classified information. The loss of U.S. COMSEC information and materials can seriously damage the national interest.

Critical Information	Specific facts about friendly intentions, capabilities, and missions needed by adversaries to plan and act to guarantee the failure of friendly mission accomplishment.
Cyber Threat	The illegal exposure to Information Technology assets and its ability to protect the confidentiality, integrity and availability of our information and operations. Cyber Threat can damages mission success and therefore must be part of your risk management processes.
DA	Department of the Army
DCSINT	Deputy Chief of Staff, Intelligence. Security and Intelligence Section located at USARC and at other headquarters.
DOD	Department of Defense
DRU	Direct Reporting Unit. An Army organization comprised of one or more units with institutional or operational support functions, designated by the Secretary of the Army, normally to provide broad general support to the Army in a single, unique discipline not otherwise available elsewhere in the Army.
EOC	Emergency Operations Center
Essential Secrecy	The condition achieved from the denial of critical information to adversaries.
FAPH	Fort AP Hill, VA
FBVA	Fort Belvoir, VA
FHNY	Fort Hamilton, NY
FISS	Foreign Intelligence Security Service
FOIA	Freedom of Information Act. Allows people to gain access to non-classified information from government agencies.
FOUO	For Official Use Only. Information that often has Social Security Numbers or other information that could harm the soldier if released.

FPCON	Force Protection Condition. Force Protection Condition. A system that provides procedures for terrorism analysts to assess the terrorist threat and for commanders to determine required security measures based on the assessed threat of terrorist attack.
Human Intelligence (HUMINT)	Collection of information by human sources for intelligence purposes. Gathered covertly by espionage agents, or overtly through information available to the general public, it is the most basic form of intelligence collection. HUMINT remains significant because it is often the only source with access to an opponent's intentions and plans.
IADC	Inter-American Defense University
Imagery Intelligence (IMINT)	Collection of information by photographic, infrared, or radar imagery. Images can be gathered either by individuals or by remote means, such as aircraft or satellite. This method is valuable because it provides analysts with clues to other areas requiring examination. The IMINT includes unauthorized duplication of documents.
Indicators	Friendly detectable actions and open source information that can be interpreted or pieced together by an adversary to derive critical information.
IO	Information Operations
JADOC	Joint Air Defense Operations Center
JBM-HH	Joint Base Myer-Henderson Hall, VA
JFHQ-NCR /USAMDW	Joint Force Headquarters National Capital Region/U.S. Army Military District of Washington
JPPSOMA	Joint Personnel Property Shipping Office Mid-Atlantic
MSC	Major Subordinate Command
Measurement and Signature Intelligence (MASINT)	Scientific and technical intelligence obtained by quantitative and qualitative analysis of data derived from technical sensors to identify any distinctive features associated with the source, emitter, or sender. It is technical in nature.

Military Deception	Actions executed to mislead foreign decision-makers, causing them to derive and accept desired appreciation of military capabilities, intentions, operations, or other missions that evoke foreign actions that contribute to the originator's objectives. Deception is an effective OPSEC measure that can be employed given prior coordination (e.g., cause adversary intelligence collection efforts to fail to target friendly missions, create confusion or misinterpretation of information obtainable from open sources).
Observables	Actions that convey indicators exploitable by adversaries but that must be carried out regardless, to plan, prepare for and execute missions.
Operations Security Compromise	The disclosure of sensitive or critical information which has been identified by the Command and all higher headquarters as jeopardizing the unit's ability to execute its mission or to adequately protect its personnel and/or equipment.
OPSEC	Operations Security. A program meant to deny our adversaries access to any critical information.
OPSEC Measure	Methods and means to gain and maintain essential secrecy about critical information.
Operations Security Planning Guidance	Guidance that serves as the blueprint for OPSEC planning by functional elements throughout the organization. It defines the critical information that requires protection from adversary, appreciations, taking into account friendly and adversary goals, estimated key adversary questions, probable adversary knowledge, desirable and harmful adversary appreciations and pertinent intelligence system threats. It also should outline tentative OPSEC measures to ensure essential secrecy.
Operations Security Vulnerability	A condition in which friendly actions provide OPSEC indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decision-making.
PAO	Public Affairs Office
TARP	Threat Awareness and Reporting Program. (Formerly known as Subversion and Espionage Directed against the Army.) (SAEDA)

SBU	Sensitive but Unclassified. Unclassified information that is readily available and which could be used against the DoD or its personnel.
SC	Subordinate Command
SCC	Service Component Command
SCI	Senior Command Installation
Sensitive Information	Any information, the loss, misuse, or unauthorized access to, or modification of which could adversely affect the national interest or the conduct of Federal programs, but which has not been specifically authorized under an Executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy (PL 100-235, 8 Jan 88).
Signals Intelligence (SIGINT)	Collection of information by interception of electronic signals from communications equipment or non-communicative devices that emit an electronic signal, such as a radar beacon. It includes interception of communication and the interception and analysis of communication between pieces of equipment (e.g., LAN).
SRU	Separate Reporting Unit
TDA	Table of Distribution and Allowances. A document authorizing equipment and personnel for a garrison unit.
TDY	Temporary Duty
TOG	United States Army Third Infantry Regiment (The Old Guard)
TUSAB	The United States Army Band
USARC	United States DoD and Army Reserve Command
Vulnerabilities	Friendly actions which provide indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decision making. Vulnerabilities exist when three conditions exist; adversary has capability to collect indicator, and adversary has time to process (report, analyze, take planning action), and the adversary must be able to react.
WHTA	White House Transportation Agency