DEPARTMENT OF THE ARMY
INSTALLATION MANAGEMENT COMMAND
HEADQUARTERS, U.S. ARMY GARRISON, FORT A.P. HILL
18436 4TH STREET
FORT A.P. HILL, VIRGINIA 22427-3114

REPLY TO
ATTENTION OF

IMPH-ZA

6 September 2012

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Commander's Policy Letter on Operations Security (OPSEC) – Policy Letter #17

1. Applicability. This policy applies to all personnel assigned, attached or visiting Fort A.P. Hill (FAPH) including tenants and partner units. Failure to comply with this policy may be punished as violations of a lawful order under Article 92 of the Uniform Code of Military Justice (UCMJ) or under other disciplinary, administrative, or other actions as applicable.

2. Proponent. Fort A.P. Hill Directorate of Plans, Training, Mobilization and Security (DPTMS), Operations, Plans and Security Division.

3. References. References are at enclosure 1.

4. Policy.

a. Operations Security (OPSEC) is the process of developing and prioritizing efficient and effective countermeasures to our enemies' ability to collect the information he needs to conduct successful operations against us. We develop these countermeasures after analyzing our threat and the Critical Information (CI) he needs to collect, and assessing our vulnerability to his collection efforts and the risk he poses to our operations.

(1) CI and Essential Elements of Friendly Information (EEFI).

(a) CI is information required by the enemy to plan and conduct operations against us. EEFI is simply CI, but worded in the form of a question.

(b) CI is generally not classified, but must be afforded a level of protection to ensure that it is not released to the public without authorization. CI in paper form should be stored in a locked drawer or container when not in use. CI may be discussed, shared or otherwise transmitted only to other personnel who need the information to complete their government assigned duties. This may include coworkers, supervisors, subordinates, contractors, first responders and other garrison, tenant or external personnel, provided that the need for information is driven by official government duties.

(2) Critical Information List (CIL)

(a) The CIL identifies information that garrison personnel are required to protect to deny the enemy the ability to conduct operations against us. It consists of Fort A.P. Hill CI, as well as higher headquarters CI and tenant unit CI. The CIL will change periodically, such as when changes in threat, vulnerability or risk occur.

(b) The CIL is at enclosure 2. The list is non-sensitive and should be given the widest distribution to ensure that the workforce is aware of the information that needs to be protected. Note the distinction: a CIL/EEFI item might be the sentence "The Location of Our Ammunition," indicating the character of information that needs to be protected. This list would be given widest distribution. The CI item, the actual location of the ammunition, "Grid XX12345678" would be sensitive, and needs to be protected from release.

(3) Threat Assessment. The primary threats against Fort A.P. Hill are:

(a) Terrorist activity

(b) Foreign intelligence collection

(c) Criminal activity

(4) Vulnerability Assessment. The Fort A.P. Hill vulnerability assessment is a controlled document, available only to personnel who require access to complete their government-assigned duties.

(a) In general, vulnerability exists where CI is observable by the enemy. Vulnerabilities can be mitigated by concealing the CI, or by preventing the enemy from observing it.

(b) Indicators are actions and information that can be pieced together to derive CI. These can include profile indicators (e.g., "Fort A.P. Hill always conducts vehicle checks at the main gate"), deviation indicators (e.g., "Fort A.P. Hill always conducts extra vehicle checks before a VIP arrives"), and tip-off indicators (e.g., "Fort A.P. Hill was conducting vehicle checks at the gate today. That's unusual. Something must be happening"). In addition to the careful control of conversation and documents, personnel must be aware of what their actions may reveal.

(5) Risk Assessment. The Fort A.P. Hill risk assessment is a controlled document, available only to personnel who require access to complete their government-assigned duties.

(6) OPSEC Countermeasures. This policy establishes baseline OPSEC countermeasures to be implemented during routine operations and exercises while at FPCON Normal and FPCON Alpha. These measures may be augmented with additional measures for specific operations, at the request of tenant, partner or visiting units, or during times of increased FPCON, in the interest of protecting CI. Fort A.P. Hill baseline OPSEC countermeasures are:

(a) OPSEC awareness training and briefings. Garrison personnel must remain vigilant against inadvertent release of critical information through non-secure radio transmissions, non-secure telephone calls, unencrypted e-mail, friendly conversations in public areas, website or web log (blog) postings, discussion forums or any other means of communicating information. This policy is not intended to discourage responsible communication or the use of social media, but rather to ensure that a compromise of CI does not place our installation at risk. Initial and annual OPSEC awareness training will be conducted for garrison personnel to ensure retention of OPSEC procedures in the workforce, provide a forum to present and answer OPSEC-related questions, receive OPSEC suggestions and illustrate recent OPSEC-related incidents, threats, vulnerabilities, problems or accomplishments.

(b) FOUO markings. For Official Use Only (FOUO) is a designation that is applied to unclassified information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA). FOUO is not a classification as FOUO information is unclassified, but is not to be released to the public without undergoing a FOIA and legal review. FOUO will be the standard marking for all unclassified products that meet one or more of the exemptions of FOIA, and which if released to the public, could cause harm to Army operations or personnel. Examples include but are not limited to: force protection, movement and readiness data, tactics, techniques, and procedures (TTPs), proprietary information and information protected by copyright, pre-decisional documents, draft publications, and information concerning security systems. FOIA exemptions are addressed in detail in AR 25-55, The Department of the Army Freedom of Information Act Program.

(c) Email encryption. Email encryption is available on the Non-Secure Internet Protocol Router Network (NIPRNet) and will be used whenever transmitting CI via email. Additionally, a message classification system is available and will be used to ensure that email recipients are aware of any CI present in email messages and attachments. (AR 530-1, para 2-1h(3)).

(d) Shredding. Fort A.P. Hill garrison offices are commonly equipped with at least two shredders. Strip shredders should be used to the maximum extent possible for the destruction of routine documents that do not contain CI, because the shredded material can be recycled. Crosscut shredders, particularly the "High Security" crosscut shredders authorized by the National Security Agency (NSA) for the destruction of classified documents, will be used to destroy non-record documents containing CI when it is no longer needed. Because the shredded material cannot be recycled, the use of crosscut shredders for unclassified, non-CI documents is discouraged. For offices without crosscut shredders or with large quantities of CI, a high-speed crosscut shredder is available for use at building 137.

(e) Disk shredding. CDROMs and DVDs containing CI may be brought to building 137 for destruction in a disk shredder and should no longer be destroyed using the strip shredders that are also used for paper, as the disk fragments render the shredded paper strips unrecyclable.

(f) OPSEC review. Products that potentially contain CI will undergo OPSEC review by a Level II-certified OPSEC Officer before they are released to the public, regardless of the form,

method or release. This includes, but is not limited to, press releases, photographs, web content, responses to FOIA, Privacy Act and other information requests, technical papers and reports, operations orders (OPORDS), contracts and contract solicitations. OPSEC review may be requested at any time through coordination with the DPTMS Plans, Operations and Security (OPS) Division and will be accomplished as quickly as operational tempo allows. Departments that frequently produce products which require OPSEC review may request OPSEC Support Element (OSE)-approved OPSEC Level II training and, upon successful certification, may conduct their own OPSEC reviews. AR 530-1, para 2-1g places responsibility for completion of an OPSEC review prior to release upon the individual who intends to release the information.

(g) OPSEC in contracting. Antiterrorism and OPSEC measures will be considered as part of the development and execution of all contracts, and applied where appropriate. Except for supply contracts under the simplified acquisition level threshold, field ordering officer actions and Government purchase card purchases, all new contracts will include a Contract Requirements Package Antiterrorism/Operations Security Review Cover Sheet, completed by the requiring agency as described in ALARACT 015-2012 and ALARACT 075-2012 effective July 1, 2012. This procedure does not mandate any specific OPSEC measure, but provides a uniform procedure for ensuring that the effectiveness and usefulness of measures is considered to mitigate any potential vulnerability created by the contract process. (AR 525-13, para 1-7a(5), para 5-19 and AR 530-1, chapter 6).

(h) Open Skies Treaty. The 1992 Open Skies Treaty is a potential OPSEC vulnerability to Fort A.P. Hill. The treaty allows signers (NATO and former Warsaw Pact nations) to conduct aerial photography of other nation's territory for the purposes of verification of treaty conditions, etc., and has the potential to compromise the activities of the garrison, and its tenants and partners. In the event of a scheduled Open Skies Treaty flight, Fort A.P. Hill OPS will initiate the procedures at enclosure 3 to determine if any High Value Activity (HVA) is being conducted, and to report HVA status to IMCOM and JFHQ-MDW/NCR. Tasked agencies will conduct their respective procedures immediately upon notification of an Open Skies mission, ensuring the protection of CI.

(i) Individual handling of OPSEC incidents. When CI or classified information appears in a public forum (as with the recent Wikileaks incident), all personnel will avoid confirming or denying the accuracy or validity of the released information. Any comment on the situation by DoD personnel undermines efforts to mitigate the damage caused by the incident. Any inquiries concerning such incidents should be directed to the Public Affairs Officer. Additionally, personnel are reminded that public posting of classified material does not automatically declassify the material. Accessing a website such as Wikileaks, whether through government IT systems or personal computers could constitute a security violation and subject individuals to investigation, loss of security clearance and other administrative or punitive action.

(j) OPSEC Working Group. The OPSEC working group will include representatives from all garrison directorates, Physical Security, Anti-terrorism, the Public Affairs office, Staff Judge Advocate, Contracting and all tenant units. Language requiring tenant unit participation in the OPSEC working group will be phased into all Inter Service Agreements (ISA) when they are

renewed, although participation in the working group will be encouraged immediately. An invitation to participate in the OPSEC working group will be extended to American Water and Rappahannock Electric Cooperative senior representatives as well.

(k) OPSEC synchronization. A combined CIL matrix for the (1) Fort A.P. Hill garrison, (2) IMCOM, (3) JFHQ-NCR/MDW and (4) tenant units is at enclosure 3. Where redundant vulnerabilities exist, measures can be applied to protect multiple echelons of CI. All four elements will endeavor to protect the CI of the other three elements as well as their own. Requests for information specifically owned by one echelon will be referred by the receiving agency to the appropriate agency's OPSEC officer, ensuring that all four elements maintain control of their own CI and simultaneously avoid the inadvertent compromise of partner agency CI.

(l) Transient units. A baseline CIL will be assumed for all transient units, and will be protected by garrison and tenant unit personnel unless otherwise instructed. Language requiring transient units to protect our synchronized CIL will be developed and included in the standard training support package. This language will also afford transient unit OPSEC officers the opportunity to present their CIL to the garrison for protection during their visit. Unless a specific CIL is presented by a transient unit, their baseline CIL will be assumed to consists of:

- Unit travel details (travel schedule, point of origin, destination, means of transportation, etc.)
- Unit training or mission ("training for deployment to Afghanistan," "conducting counterinsurgency training," "learning mine-removal procedures," etc.)
- Unit Modified Table of Organization and Equipment (MTOE) or Table of Distribution and Allowances (TDA) details (unit strength, weapons, night vision equipment, types of vehicles, etc.)

(m) Release of information to external agencies. Cooperation and information exchange with local, state and federal agencies is necessary for the success of those agencies and Fort A.P. Hill's mission. In the interest of furthering our respective missions, CI may be shared with external agencies on a case-by-case basis, provided that they acknowledge in writing that the CI they receive will be afforded a level of protection equal to what it receives at Fort A.P. Hill, and will not be forwarded any further without the written approval of the originating office at Fort A.P. Hill.

5. The implementation of these OPSEC measures protects our critical information, reduces vulnerabilities and risk, and protects our families, our community, our workplace and our Warriors.

6. Point of contact is the OPSEC Manager at (804) 633-8982/8304.

PETER E. DARGLE
LTC, AR
Commanding

Encls
1. References
2. Critical Information List and Sync Matrix
3. Fort A.P. Hill Open Skies Treaty Notification Guidance

DISTRIBUTION:
A

Enclosure 1

References

a. AR 530-1, Operations Security (OPSEC), 19 April 2007.

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

c. ALARACT 015/2012, Use of an Antiterrorism/Operations Security (AT/OPSEC) In Contracting Cover Sheet for Integrating AT/OPSEC into the Contract Support Process, 24 January 2012

d. ALARACT 075/2012, Antiterrorism Quarterly Theme – Integrating Antiterrorism and Operations (Sec)urity (OPSEC) into the Contract Support Process (3Q/FY12)

e. ALARACT 271/2010, OPSEC Emphasis on Protection of C-IED and IEDD Critical Information

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

g. National Security Decision Directive Number 298, National Operations Security Program, January 22, 1988.

h. DoD 5205.02-M DoD Operations Security (OPSEC) Program Manual, 3 November 2008.

i. DoDD 5202.02E, DOD Operations Security (OPSEC) Program, 20 June 2012.

j. AR 381-12, Threat Awareness and Reporting Program, 4 October 2010.

k. AR 525-13, Antiterrorism, 11 September 2008.

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

m. AR 25-2, Information Assurance, 23 March 2009.

n. FM 3-13, Information Operations: Doctrine, Tactics, Techniques, and Procedures, 28 November 2003.

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

p. Commander's Policy Statement on Social Media – Policy Memorandum #32, 20 July 2011.

Enclosure 2

Critical Information List and Sync Matrix

(This enclosure contains information that is also contained Annex A of the Fort A.P. Hill OPSEC Plan, which will be updated simultaneously with this Enclosure)

Critical Information / Essential Elements of Friendly Information
What are the details of upcoming operations (schedules, locations, participants, etc.)?
What are the details of higher headquarters, tenant, partner and transient units (schedules, strength, location, capabilities, ranges used, home station information, equipment, etc.)?
What are the details of communication systems and procedures (telephones, computer network, radios, communication facilities, etc.)?
What are the details of Physical Security, Force Protection and Law Enforcement efforts (access control measures, police schedules, police strength, police capabilities, etc.)?
What are higher headquarters, garrison, tenant and partner Personally Identifiable Information (PII) (social security numbers, home addresses, telephone numbers, dates of birth, etc.)?
What are the details (location, vulnerability, etc.) of critical infrastructure (water, sewer, electricity, fuel, ammunition)?
What are the details concerning the schedule, itinerary, and location of VIPs and High Risk Personnel (HRP)?
What are our intelligence capabilities, limitations or vulnerabilities?
What are the details of Counter-Improvised Explosive Device (C-IED) or Improvised Explosive Device-Defeat (IEDD) training, operations or equipment?

Enclosure 3

Open Skies Treaty Notification Procedures

1) **SITUATION.**

a) Enemy Forces. N/A

b) Friendly Forces. N/A

c) Weather. N/A

d) Attachments and Detachments. N/A.

2) **MISSION**. Upon notification of a scheduled Open Skies Treaty flight, Fort A.P. Hill OPS will initiate reporting procedures to determine if any High Value Activity (HVA) is being conducted, and to report HVA status to IMCOM.

3) **EXECUTION**.

a) The 1992 Open Skies Treaty is a potential OPSEC vulnerability to Fort A.P. Hill. The treaty allows signers (NATO and former Warsaw Pact nations) to conduct aerial photography of other nation's territory for the purposes of verification of treaty conditions, etc., and has the potential to compromise the activities of the garrison, and its tenants and partners. These procedures will ensure the protection of Critical Information (CI).

b) Open Skies Treaty Notification procedures will occur in five phases.

i) Phase I is the Notification Phase. During this phase, OPS division contacts the offices and tenants listed below to report the Open Skies Treaty Overflight information.

Open Skies Treaty Overflight information	Contacted offices and tenants
o Date/time group (local) for the start of overflight window o Date/time group (local) for the end of overflight window o HVA criteria o Reporting procedures o Reminder that negative responses are necessary o Alternate point of contact, as necessary o Date/time group (local) for submission suspense o Contact information for report submission (classified and unclassified)	o NSWG2 o NSWC IH o NVESD (DZ) o NVESD (71A) o AWG o EOD School o (Other tenants and partner units may be added to this list upon request) o DPTMS Aviation o DPTMS Range Operations

ii) Phase II is the Schedule Scrub Phase. During this phase the contacted offices and tenants will determine whether any High Value Activity (HVA) meeting the criteria below is presently scheduled. DPTMS Aviation and DPTMS Range Operations will coordinate this schedule scrub with transient units scheduled to conduct training at Fort A.P. Hill in the specified period.

(1) HVA must meet one or more of the following criteria:

(a) Activity or event that requires implementation of restricted/hazardous airspace to support the planned HVA.

(b) Activity or event that cannot be postponed or cancelled without the United States Government incurring substantial monetary cost.

(c) Activity or event that cannot be concealed and observation will cause irreparable damage to national security.

(d) Activity or event that takes advantage of a unique set of chronological or meteorological circumstances which cannot be duplicated.

(e) The Garrison Commander believes that special circumstances apply and fully explains these circumstances.

iii) Phase III is the Internal Reporting Phase. During this phase the contacted offices will report all HVA to OPS. Note that negative responses are required. Information will be reported in the following format:

(1) Organization conducting the HVA, to include contact information.

(2) Description of the HVA (if the HVA is classified, report either in person to the OPS division, using a STE telephone in "secure" mode", or via Secure Internet Protocol Router (SIPR).

(3) Date/Time of the HVA.

(4) Location (Latitude/Longitude in degrees: minutes: seconds) of the center of mass for the HVA and designator of the Special Use Airspace (SUA) if used.

(5) Whether rescheduling is possible.

(6) Description of the impact caused by rescheduling/cancellation of the HVA.

(7) Cost of rescheduling/cancellation of the HVA.

(8) Additional remarks/Special circumstances.

(9) Contact information for the individual submitting the report, if different from #1.

iv) Phase IV is the External Reporting Phase. During this phase, OPS will compile all HVA and report to IMCOM (copy to JFHQ-NCR/MDW). HVA will be reported via SIPR. Negative responses may be reported via NIPR. Reports will be in the following format:

(1) Name of reporting Installation/Activity.

(2) Date/Time (In Zulu) of HVA Report.

(3) Point of Contact/Contact telephone numbers (Com/DSN).

(4) Description of the HVA.

(5) Date/Time (In Zulu) of the HVA.

(6) Location (Use Latitude/Longitude in degrees: minutes: seconds) of the center of mass for the HVA and designator of the Special Use Airspace (SUA) if used.

(7) Description of the impact caused by rescheduling/cancellation of the HVA.

(8) Cost of rescheduling/cancellation of the HVA.

(9) Additional remarks/Special circumstances

v) Phase V is the After Action Review (AAR) phase. During this phase, OPS will query the contacted offices via email to determine if there are any suggestions to make this process proceed more efficiently. Negative responses to the AAR phase are not required.

(1) Language requiring compliance with these procedures will be developed and implemented upon renewal of Inter Service Agreements (ISA).

(2) All contacted activities will either report negative HVA, or will submit the following HVA information to OPS:

(3) OPS will report HVA (including negative responses) to IMCOM and JFHQ-NCR/MDW.

4) Service and Support. N/A.

5) Command and Signal N/A.