DEPARTMENT OF THE ARMY
UNITED STATES ARMY JAPAN
UNIT 45005
APO AP 96343-5005

APAJ-OPP (25-30mm) 15 DEC 2023

COMMAND POLICY MEMORANDUM 23-28

FOR SEE DISTRIBUTION

SUBJECT: United States Army Japan (USARJ) Operations Security (OPSEC)

1. References.

a. Army Regulation 530-1 Operations Security

b. Army Regulation 25-400-2, Army Records Management Program

c. U.S. Army Pacific Regulation 525-2, Protection

2. Records Management. All records created as a result of this policy will be managed in accordance with reference b and the USARPAC Records Management Program Policy Memorandum #23-01. This Command Policy Memorandum rescinds and replaces Command Policy Memorandum 21-26.

3. Purpose. Determine indicators and vulnerabilities that adversary intelligence systems might obtain and to be establish the USARJ OPSEC program to provide guidance and assign responsibilities throughout USARJ.

4. Applicability and Scope. This policy applies to all Department of the Army (DA) Soldiers, DA Civilians (DAC), Department of Defense (DoD) Contractors, Host Nation employees, and command sponsored dependents with Status of Forces Agreement (SOFA) status assigned or attached to USARJ and other units and activities on any U.S. Army installation in Japan.

5. Background. It is DoD policy to establish and maintain OPSEC programs to ensure national security-related missions and functions are protected. The OPSEC process is a systematic method used to identify, control, and protect critical information related to military tactics, techniques, and procedures (TTPs), capabilities, operations, and other activities.

a. OPSEC is a commander's program; commanders at all echelons are responsible for ensuring their unit, activity, and personnel plans, integrates, and implements OPSEC to protect critical information in every phase of all operations, exercises, and activities.

b. OPSEC is an operations function that protects critical information and requires close integration with other security programs that protect classified information. Failure to properly protect critical information can result in serious injury or death; damage to systems, equipment, and facilities; loss of sensitive technologies; and mission failure.

c. OPSEC is a primary function under the Army Protection Program (APP) and is aligned with mutually supporting functions of Antiterrorism (AT), Emergency Management (EM), Mission Assurance (MA), Insider Threat (InT), Physical Security (PS), Information Security (INFOSEC), and Personnel Security (PERSEC).

6. Roles and Responsibilities.

a. OPSEC is everyone's responsibility. However, the success or failure of OPSEC is ultimately the responsibility of the commander. All personnel who have access to sensitive, critical, or classified information must understand what constitutes the unit critical information, the threats to critical information, and the measures to implement to protect critical information.

b. USARJ G-34 Protection is the Office of Primary Responsibility (OPR) for OPSEC, however, the entire staff must integrate OPSEC into planning and execution of all USARJ operations and activities.

7. Concept of Implementation.

a. USARJ Headquarters and subordinate organizations integrate OPSEC into the planning, preparation, and execution of all exercises, activities, operations, and missions executed during operations to protect information contained in Operations Plans (OPLANs), Contingency Plans (CONPLANs), Operation Orders (OPORDs), and other supporting plans and orders.

b. In accordance with (IAW) AR 530-1, paragraph 2-18 a. (4), an OPSEC program includes, at a minimum, OPSEC Officer appointment orders and OPSEC plan, unit, or activity's threat assessment, developed Critical Information List (CIL) (approved by commander and disseminated), vulnerability assessment, risk assessment, and (signed) OPSEC measures to protect critical information. This OPSEC Command Policy Memorandum, along with the enclosed USARJ OPSEC Standard Operating Procedure (SOP), constitute the USARJ OPSEC Program.

c. OPSEC measures must be specifically included in contracts. All USARJ contracts will include the U.S. Army Antiterrorism (AT) / OPSEC Coversheet discussed in Section 2-2 of the USARJ OPSEC SOP.

d. OPSEC measures must be part of all inspections, local or Higher Headquarters Assessments (HHA).

e. The USARJ OPSEC Program Manager (PM) and/or OPSEC Officer(s) will conduct a command OPSEC risk assessment annually using the OPSEC risk assessment process outlined in Section 3 of the USARJ OPSEC SOP to provide the Commander an assessed level of acceptable OPSEC risk. USARJ Staff OPSEC Coordinators will assist the USARJ OPSEC PM in the development of the annual risk assessment or as directed.

f. Staff OPSEC Coordinators will participate in the OPSEC Working Group and assist the USARJ OPSEC PM as directed.

8. OPSEC Compromises. OPSEC compromise is the disclosure of sensitive and/or critical information that jeopardizes a unit's ability to execute its mission or to adequately protect its personnel and/or equipment or negatively impacts national security. In the event of an OPSEC compromise, personnel will:

a. Immediately notify their OPSEC representative and security manager of the OPSEC compromise.

b. NOT reference the location / medium of compromise outside of intragovernmental or authorized official methods of communication.

c. NOT respond to inquiries to confirm or deny the validity of information that has been compromised.

d. For OPSEC compromises which include Personally Identifiable Information (PII):

(1) Notify their Privacy Official, and if cyber-related to their Information Technology division as well.

(2) If the actual or suspected incident involves PII as a result of a contractor's actions, the contractor must also notify the Contracting Officer Representative (COR) immediately.

(3) If the incident involves a Government-authorized credit card, the issuing bank should be notified immediately.

(4) Submit "US-CERT Incident Reporting System" report https://www.us-cert.gov/forms/report.

e. Personnel who fail to comply with orders, directives or policies to protect critical and sensitive information may be subject to administrative actions or discipline under the Uniform Code of Military Justice (UCMJ) or other applicable rules and regulations, as appropriate.

f. Personnel not subject to the UCMJ who fail to protect critical and sensitive information from unauthorized disclosure may also be subject to administrative, disciplinary, contractual, or criminal action.

g. With regard to contractors, OPSEC compromises and discipline for such compromises must be reported through the COR for appropriate action.

h. With regard to federal Civilian employees, disciplinary action associated with OPSEC compromises will be reported through the Civilian Personnel Advisory Center (CPAC) to the employee's supervisor for appropriate action.

9. Coordinating Instructions.

a. USARJ Staff Directorates, Subordinate and Tenant Commands will designate an OPSEC Officer or OPSEC Coordinator to support OPSEC requirements on behalf of their directorate or command. The name and contact information of the designee will be provided to the USARJ OPSEC PM upon the publication of this policy, annually thereafter, and upon any change of designated OPSEC Officer.

(1) The appropriate rank/grade level for an OPSEC PM and OPSEC Officers must be followed IAW AR 530-1. Activities and other organizations that do not employ a traditional military command structure will determine the appropriate rank/grade level for their OPSEC officers. USARJ Staff Directors may determine the appropriate rank/grade level for their designated OPSEC Officer or Coordinator. Contractors do not have authority over U.S. Unformed personnel or DACs and will not be assigned as an OPSEC Officer or Coordinator. Likewise Host Nation employees will not be assigned as an OPSEC Officer or Coordinator. However, Contractors and Host Nation employees may perform OPSEC duties in a supporting capacity to a properly assigned OPSEC designee. OPSEC PMs, OPSEC Officers and OPSEC Coordinators must have appropriate security clearance.

(2) Army Commands (ACOM), Army Service Component Commands (ASCC), DRU, Installation, Corps. An experienced commissioned officer (at least O4 or W3), or a DAC equivalent.

(3) Division. O3 or above, W2 or above, noncommissioned officer (NCO) (E8 or above), or DAC equivalent.

(4) Brigade. O3 or above, warrant officer, NCO (E7 or above), or DAC equivalent.

(5) Battalion. O2 or above, warrant officer, NCO (E6 or above) or DAC equivalent.

(6) Commanders at all levels can approve exceptions to required grade as authorized within Army Regulation.

b. All Army Personnel in Japan will.

(1) Know and protect unit critical information.

(2) Comply with established OPSEC programs and security practices to protect critical information.

(3) Be aware of current adversary intelligence collection threats.

(4) Report any request by unauthorized personnel to solicit sensitive or critical information immediately to the nearest counterintelligence office and the chain of command.

(5) Ensure compliance with AR 350-1, Ref. a, Appendix L, titled "Information That May Be Exempt from Release under the Freedom of Information Act (FOIA)," before releasing any information requests.

c. Directors and Commanders will.

(1) Designate and assign in writing an OPSEC Officer or OPSEC Coordinator.

(2) Identify critical information, indicators, and OPSEC measures to protect critical or sensitive information specific to the unit's mission. Ensure the Unit's CIL is nested within Higher Headquarters (HHQs) CIL.

(3) Know their organization's critical information, where it is located, who is responsible for it, how to protect it, and why it needs to be protected.

(4) Plan, integrate, and implement OPSEC measures to protect their command's critical information in every phase of all operations, exercises, tests, or activities.

(5) At battalion and higher echelons develop a CIL for the Commander's approval and document it in a command OPSEC SOP and training.

(6) Review and update the unit CIL annually.

(7) Ensure compliance with Section 2-3 of the USARJ OPSEC SOP (USARJ Policy on Shredding of ALL Printed Materials).

d. The OPSEC review is a documented evaluation of information or visual products intended for public release to ensure protection of critical and/or sensitive information. The unit OPSEC officer or OPSEC Level II trained Public Affairs Officer (PAO) representative must review all products or information prior to release to the public including information contained within FOIA, Websites, critical infrastructure program documents and contracts.

e. IAW AR 530-1 Paragraph 2-18, Ref. a., all Army units, activities, agencies, installations, and staff organizations at battalion-level and higher, including equivalent table of distribution and allowances organizations will have functional, active, and documented OPSEC program, reviewed annually (within one year) and will include the establishment of a CIL and completion of the 5 Step OPSEC process.

f. Commanders will provide oversight of the OPSEC program and ensure Commander's Inspection Program (CIP) and Operational Inspection Program (OIP) inspections include comprehensive OPSEC program assessment. Annual checks may include self-assessments, program reviews as part of inspector general inspections, or HHAs specifically addressing OPSEC. The OPSEC assessment determines the overall OPSEC posture and degree of compliance by the assessed organization with applicable OPSEC plans and programs. OPSEC assessments will only be conducted by assigned OPSEC PM and / or OPSEC Officer and appropriate subject matter experts from throughout the organization.

10. Training Requirements. IAW AR 530-1, Commanders and equivalent leadership will ensure all personnel receive appropriate OPSEC training based on their duties or position. Required training is: Level I certification training, Level II certification training, and training for those who interact with the public (Web masters, PAOs, FOIA, speech writers, and Family Readiness Group (FRG) volunteers). Commanders will also provide OPSEC training guidance annually as required.

a. OPSEC Level 1 Training (Initial OPSEC Awareness Training). All personnel must receive initial training within the first 30 days after arrival to the organization. This training should be conducted as part of an initial-entry briefing or newcomers briefing. Unit OPSEC officers must track attendance and ensure that all personnel receive initial OPSEC training. The initial training will address the following:

(1) The difference between OPSEC and other security programs is how OPSEC complements traditional security programs to maintain essential secrecy of U.S. Military capabilities, intentions, and plans.

(2) The definition of critical information.

(3) Adversary collection techniques.

(4) The organization's critical information and countermeasures.

(5) The responsibility of each person to safeguard critical information.

(6) If the actual or suspected incident involves PII occurs as a result of a contractor's actions, the contractor must also notify the COR immediately.

b. Continuous OPSEC Awareness Training. OPSEC awareness training must be continually provided to the workforce, reemphasizing the importance of sound OPSEC practices. This training may include periodic OPSEC news releases in local command publications, OPSEC posters in unit areas, OPSEC information bulletins on unit bulletin boards, and OPSEC awareness briefings. Training should also include: recognition of the OPSEC Officer, where the CIL is posted, where Soldiers can find OPSEC measures, and what the Soldiers' and their families' responsibilities are. Training should also include current threats and their collection capabilities and trends.

(1) IAW AR 350-1, Ref k., Table F-1, at a minimum, all U.S. Army Pacific (USARPAC) personnel must receive an annual OPSEC awareness briefing provided by the organization's OPSEC Officer. This training must include a portion of instruction updated with current information and adapted to the organization's specific mission, area of operations and critical information.

(2) Commanders will ensure OPSEC training is provided during pre and post-deployment operations to deploying and redeploying individuals/units and to FRGs. Units should tailor training IAW specific mission parameters.

(3) Personnel who publish or release information to the public or on external official presence (EOP), post information to any public venue, or who regularly interact with the public must complete OPSEC Level II training and the following computer-based training available at https://iatraining.us.army.mil/: OPSEC for EOP Operators, Web Content and OPSEC Certification, and Social Networking v2.1. All OPSEC Officers must successfully complete the OPSEC Level II training course and designees should contact the USARJ OPR within 30 days of assignment to secure a seat in the next available TRADOC Mobile Training Team course.

c. OPSEC Level II certification training. The HQDA OPSEC Officers Course will train and prepare personnel to manage an OPSEC program and advise the commander on all OPSEC matters.

11. OPSEC Process. The OPSEC process applies to all phases of an activity, function, or operation and is used in the development of OPSEC plans and annexes. The five fundamental steps are: Identification of Critical Information, Analysis of Threats, Analysis of Vulnerabilities, Assessment of Risk, Application of OPSEC measures.

a. Identification of Critical Information. The purpose of this step is to determine what information needs protection. Critical information is information important to the successful achievement of U.S. objectives and missions, or which an adversary may use to harm U.S. and friendly personnel or hinder operations. Critical information consists of specific facts about friendly capabilities, activities, limitations (includes vulnerabilities), and intentions needed by adversaries for them to plan and act effectively so as to degrade friendly mission accomplishment. All units must employ OPSEC measures to protect this information. All subordinate unit CILs are tailored to the unit specific mission and situation and will include all elements of the USARPAC CIL. The approved USARJ CIL is found in Section 2 of the USARJ OPSEC SOP and will be reviewed and updated annually.

b. Analysis of Threats. The purpose of this step is to identify adversary collection capabilities against critical information. Adversary collection activities target actions and open-source information to obtain and exploit indicators that will negatively impact the mission. OPSEC indicators are friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information.

c. Analysis of Vulnerabilities. The purpose of this step is to identify possible OPSEC measures for each vulnerability. The most desirable measures provide needed protection at the least cost to operational efficiency. Select at least one OPSEC measure for each vulnerability. Some measures may apply to more than one vulnerability.

d. Assessment of Risk. The purpose of this step is to identify and select OPSEC measures for implementation. The OPSEC Officer recommends to the Commander the OPSEC measures that he or she believes the Commander should implement. The Commander must balance the risk of operational failure against the cost of OPSEC measures and consider the following.

(1) What is the likely impact of an OPSEC measure on operational efficiency?

(2) What is the probable risk to mission success if the unit does not implement an OPSEC measure?

(3) What is the probable risk to mission success if an OPSEC measure does not work?

(4) Decide which OPSEC measures to implement, when to implement, and when to terminate implementation.

(5) Check the interaction of OPSEC measures. Ensure that a measure to protect a specific piece of critical information does not unwittingly provide an indicator of another.

(6) Coordinate OPSEC measures with Protection functions (i.e. Physical security, information security, etc.) and the other elements of Information Operations.

(7) The Commander may decide on a no-measures alternative. This is acceptable if the OPSEC process was used to determine that no critical information requires protection or that the costs outweigh the risks. However, that decision must be documented for future reference.

e. Implement Appropriate OPSEC measures. The purpose of this step is to apply OPSEC measures to protect critical information. The OPSEC annex of each operations order will address the implementation of specific OPSEC measures.

f. The command must also realize it may have specific responsibilities assigned in AR 350-1 and must adhere to those unless granted exception by appropriate authority.

g. Commands required to conduct annual an OPSEC risk assessment may use the five step OPSEC Risk Assessment process as outlined above or may use the OPSEC Risk module within DoD's Enterprise Risk Management System (EPRM) found on SIPR. For information regarding EPRM access and use, contact the USARJ OPSEC PM.

h. As part of the OPSEC process, HQDA requires an OPSEC Report submitted annually. The purpose of this report is to identify Army OPSEC challenges and to chart a way ahead that feeds resourcing justifications and decisions. Subordinate commands should forward concerns to the program manager; a list of representative data elements are provided in AR 350-1, appendix I for reference.

12. OPSEC Coordination. The application of OPSEC measures is a continuous cycle that includes evaluating intelligence and counterintelligence (CI) reports, public media disclosures, web site reviews, integrated systems security monitoring, and feedback reports on OPSEC measures. Directors/Commanders will:

a. Ensure intelligence and CI capabilities (if assigned), provide intelligence and CI support to the command's OPSEC program. CI counters or neutralizes the adversary's intelligence collection efforts through collection, counterintelligence investigations, operations, analysis, and production, and functional and technical services. When this is not practical or possible, forward OPSEC-supporting intel and/or CI requirements to the next higher OPSEC officer.

b. Ensure the public affairs review process includes OPSEC to prevent the release of sensitive and/or critical information which includes information exempt from public disclosure per doctrine listed in AR 350-1, or that is subjected to export controls. A public affairs-qualified NCO / DAC / Officer may conduct this review. If unsure the information is releasable, the PAO should consult the owner of the information.

c. Ensure all OPSEC PMs/Officers/Coordinators, information operations (IO) professionals, PAOs, FOIA officers, speechwriters, contracting specialists, Foreign Disclosure Officers (FDO) and personnel responsible for the review and approval of information intended for public release receive OPSEC training tailored to their duties. The popularity and availability of a social networking sites, photo sharing, Web log (blogs), and so forth have greatly increased the risk of inadvertent disclosures of sensitive, critical and possibly classified information (alone or through compilation). Access to the internet via mobile devices in addition to traditional workstations reduces the amount of reaction time and increases risk to sensitive and/or critical information.

d. Mission owners of Defense Critical Infrastructure Program (DCIP) will identify and protect, using OPSEC measures, critical information related to DCIP plans and programs and to integrate DCIP into OPSEC assessments and surveys as needed.

e. Identify OPSEC resource requirements through the command's program objective memorandum process or (subordinate unit) request through proper channels.

13. Action Officer for this Command Policy Memorandum is the USARJ OPSEC Program Manager, Mr. Marcus D. McAllister at 315-262-8177, or via email at marcus.d.mcallister.civ@army.mil.

DAVID B. WOMACK
MG, USA
Commanding

Encl
USARJ OPSEC SOP

DISTRIBUTION:
A
B
Special

Operations Security

PSEC

Protect USARJ’s Information!

Summary. This Standard Operating Procedures (SOP) provides Command policy and procedures for the establishment and execution of Operations Security (OPSEC) programs within United States Army Japan (USARJ), under the provisions of Army Regulation (AR) 530-1 and other referenced documents.

Effective Date: 01 November 2023

Applicability. This SOP applies to all USARJ, subordinate, OPCON, those who are TACON for Force Protection (FP) to Commander (CDR) USARJ, and tenant units on any U.S. Army installation in Japan.

Suggested Improvements. The Office of Primary Responsibility for this SOP is G-34 Protection and the Action Officer is the USARJ OPSEC Program Manager. Users are invited to send comments/suggestions USARJ OPSEC Program Manager, ATTN: G-34 Protection, Unit 45005, APO AP 96343-5005.

CONTROLLED UNCLASSIFIED INFORMATION
CONTROLLED BY: USARJ (G-34 PROTECTION)
CUI CATEGORY(IES): OPSEC
LIMITED DISSEMINATION CONTROL: REL TO USA, JPN
POC: OPSEC PROGRAM MANAGER, DSN 315-262-8177

TABLE OF CONTENTS

SECTION 1 – USARJ OPSEC PROGRAM

SECTION 2 – CRITICAL INFORMATION AND OPSEC MEASURES

SECTION 3 – OPSEC RISK ASSESSMENT

SECTION 4 - REPORTS

RECORD OF CHANGES

Version	Date of Change	Description of Changes	Made By

SECTION 1 – USARJ OPSEC PROGRAM

1-1REFERENCES

1. CJCS INST 3213.01B, Joint Operations Security

2. DoDD 5205.2E, DoD Operations Security Program

3. Joint Pub 3-13.3, Joint Doctrine for Operations Security

4. Army Regulation 360-1, Army Public Affairs Program

5. Army Regulation 525-2, Army Protection Program

6. Army Regulation 530-1, Operations Security

7. USPACOM Instruction 0302.1

8. USARPAC Regulation 525-2 Protection

9. USARPAC ORDER 20-03-063, OPSEC Plan

10. USARJ OPORD 23-08-009, USARJ Insider Threat Program

11. USARJ Command Policy Memorandum 21-26, OPSEC

SECTION 1 – USARJ OPSEC PROGRAM
1-2 OPSEC DEFINITIONS

1. Operations Security. As defined in Department of Defense Directive (DoDD) 5205.02E, OPSEC is a process of identifying critical information and analyzing friendly actions attendant to military operations and other activities to —

a. Identify those actions that can be observed by adversary intelligence systems.

b. Determine indicators and vulnerabilities that adversary intelligence systems might obtain to be able to interpret or piece together to derive critical information in time to use against U.S. and/or friendly missions and poses an unacceptable risk.

c. Select and execute measures that eliminate the risk to friendly actions and operations or reduce to an acceptable level.

2. Critical Information. Critical information, formerly known as essential elements of friendly information, is defined as information important to the successful achievement of U.S. objectives and missions, or which may be of use to an adversary of the United States.

a. Critical information consists of specific facts about friendly capabilities, activities, limitations (includes vulnerabilities), and intentions needed by adversaries for them to plan and act effectively so as to degrade friendly mission accomplishment.

b. Critical information is information that is vital to a mission that if an adversary obtains it, correctly analyzes it, and acts upon it; the compromise of this information could prevent or seriously degrade mission success.

c. Critical information can either be classified or unclassified depending upon the organization, activity, or mission. Critical information that is classified requires OPSEC measures for additional protection because it can be revealed by unclassified indicators. Critical information that is unclassified especially requires OPSEC measures because it is not protected by the requirements pertaining to classified information. Critical information can also be an action that provides an indicator of value to an adversary and places a friendly activity or operation at risk.

3. Critical Information List (CIL). A list of critical information that has been fully coordinated within an organization and approved by the Commander, and is used by all personnel in the organization to identify unclassified information requiring application of OPSEC measures.

4. OPSEC Measures. Identified and executable actions that eliminate vulnerabilities to Critical Information or reduce risk of compromise to an acceptable level.

5. OPSEC Program Manager. An individual trained in OPSEC responsible for the development, organization, and administration of an OPSEC program at ACOM, ASCC, DRU, garrison, and corps and higher.

6. OPSEC Officer. An individual trained in OPSEC responsible for the development, organization, and administration of an OPSEC program at division-level and below.

7. OPSEC Coordinator. An individual trained in OPSEC who assists the OPSEC Program Manager or OPSEC Officer in the development, organization, and administration of the command's OPSEC program.

8. Insider. An Insider is a person who has, or once had authorized access to classified or controlled unclassified Department of Defense (DoD) information, or who has current authorized access to a DoD facility, information network, or other DoD resource.

9. Insider Threat. An Insider threat is a threat to the DoD by an insider who, wittingly or unwittingly commits an act or displays a behavior that either will or is reasonably likely to cause a loss, degradation of, or harm to DoD personnel, information networks, resources, or capabilities, and thereby damage the security of the United States. This threat includes damage to the US through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities by acts of violence in the workplace.

10. OPSEC Compromise. An OPSEC compromise is the disclosure of sensitive and/or critical information that jeopardizes a unit's ability to execute its mission or to adequately protect its personnel and/or equipment or affects national security.

SECTION 2 – CRITICAL INFORMATION AND OPSEC MEASURES

2-1 USARJ CRITICAL INFORMATION LIST

1. Critical information, formerly known as essential elements of friendly information, is defined as information important to the successful achievement of U.S. objectives and missions, or which may be of use to an adversary of the United States.

2. All elements of the USARJ Critical Information List (CIL) are aligned with Operations, Plans, Communications, Intelligence, Logistics and Resource Management, Personnel, and information subject to compromise via Internet Based Media.

3. USARJ Critical Information:

a. Operations:

(1) Key Assets, Forces & Weapons Systems. Critical Information relating to Task Critical Assets; Pre-positioned Stock; Unit Status Report and Army Readiness Management data; task organization, disposition, composition, strength and combat readiness posture of assigned or transient forces; status and/or limitations of personnel, equipment, and weapons systems and key contingency concepts processes.

(2) Standard Operating Procedures.

(3) Specific aspects and changes of Force Protection Conditions.

(4) Details and locations of operations and exercises in support of assigned missions including capabilities, operational units participating, or their state of readiness.

(5) Exercise and/or inspection postures, results or corrective action planning.

(6) Any information revealing vulnerabilities of facilities, assets or critical infrastructure.

(7) The Random Antiterrorism Measures Program.

(8) Policies and information regarding Rules of Engagement (ROE), to include the use of weapons and electronic weapons or systems. Identification, strength, combat readiness posture of assigned/aligned base defense forces, alert status, response times, and schedules.

(9) Defense Critical Infrastructure. Critical Information relating to Defense Critical Infrastructure may include, but is not limited, specifics to the following: electric power systems; communication or automation nodes/lines; data centers; ammunition storage sites; hospital/medical facilities; roads/intersections; fuel points; petroleum, oil, and lubricant tank farms; headquarters, operations, intelligence, maintenance, or first responder facilities; supervisory control and data acquisition; industrial control systems. Location, schematics, capabilities, protection measures, vulnerabilities, and degradation of critical infrastructure.

b. Plans:

(1) Changes in mission(s) and/or tasking.

(2) Deployment or Mobilization dates or timelines.

(3) Specific information on schedule of forces, equipment, or staging locations.

(4) Security Classification of operations, plans, programs, or projects.

(5) Assessments or reports relating to assets or critical Infrastructure.

(6) Evacuation routes, procedures, and rally points.

(7) Intended operational changes before public announcement.

(8) Specifics about access control, physical security capabilities, force protection assets, implementing conditions, random measures, schedules, installation arming locations, unofficial special events (i.e. high school graduations), unpublicized off-installation movements, building evacuation plans and procedures, and emergency action drills.

c. Communications:

(1) Capabilities, configuration, security measures, limitations, status, upgrades, or proposed changes related to communication systems, to include networks, transmission systems, relay stations, and associated equipment.

(2) Technical system architectures, capabilities, vulnerability information, and security assessment reports related to C2 systems or National Security Systems.

(3) Security, network architecture, topology, infrastructure, infrastructure design, and security risk assessment results of USARJ information technology.

(4) Network architecture diagrams or documents.

(5) Information revealing a communications security weakness or physical security weaknesses.

(6) Computer passwords, user IDs, Personal Identification Numbers (PINs) and / or network access paths.

(7) Security authorization documentation including data provided to support Authorization to Operate or Connect decisions.

(8) Data collected in order to grant access to USARJ information technology e.g., System Authorization Access Request forms.

d. Intelligence:

(1) Intelligence sources or methods of gaining intelligence; analytical methods and processes.

(2) Intelligence assessments, maps, and locations of intelligence targets.

(3) Intelligence, surveillance, and reconnaissance resources.

(4) Counterintelligence capabilities.

(5) Gaps and limitations in intelligence.

(6) Counter surveillance capabilities.

e. Logistics and Resource Management:

(1) Time Phased Force Deployment Data and Reception, Staging, Onward movement, and Integration details

(2) Speed of deployment/redeployment of forces.

(3) Contracting and funding data.

(4) Deployment of special equipment, readiness, or supply status.

(5) Status of pertinent ground, air, and sea lines of communications, locations and capabilities of storage depots, ports, airfields, and hospitals.

(6) Changes or shortages in equipment and/or readiness status that may impair mission capabilities.

(7) Emergency action/repairs to preserve habitability, safety or security of USARJ infrastructure.

(8) New equipment capabilities and/or limitations.

(9) Specific contract criteria stated in classified contracts or identification of Special Access elements within a contract or program.

(10) Emergency requisition of funds (or unexpected loss of funding) disclosing details of daily and/or contingency operations.

(11) Real property information including blueprints, detailed diagrams, facility utilization studies, floorplans, maps or photos of base layouts and geospatial data.

f. Personnel:

(1) Personally Identifiable Information (PII).

(2) Identification and relation of command personnel with security badge, security clearances or access, and special projects.

(3) Protected health Information (Immunization, medical requirements, health status, and deficiencies.)

(4) Location, itineraries, and travel modes of key USARJ military and civilian personnel.

(5) Manpower gains or losses associated with contingency operations or exercises.

(6) Individual or collective training deficiencies impairing mission essential functions.

(7) Location, itineraries, and travel modes of Distinguished Visitors to USARJ.

(8) Lists of critical or executive personnel with USARJ issued mobile devices.

g. Critical information subject to compromise via Internet Based Media:

(1) Personally Identifiable Information (PII).

(2) Full organizational rosters and telephone directories.

(3) Contingency plans and/or continuity of operations.

(4) Architectural or floor plans, diagrams of an organization’s building property, or installation.

(5) Pictures or videos containing any security features. (e.g., guard shack, barriers, security tactics, techniques or procedures, access badges, safes, locking mechanisms, etc.)

SECTION 2 – CRITICAL INFORMATION AND OPSEC MEASURES
2-2 USARJ OPSEC VULNERABILITIES

1. An OPSEC vulnerability creates the conditions which allow an adversary to collect critical information.

2. USARJ OPSEC vulnerabilities:

a. Personnel who lack an understanding of OPSEC.

b. Complacency in OPSEC policy enforcement.

c. Discussion of sensitive information in unsecured / open areas.

d. Mishandling of sensitive / CUI / PII (Spillage or compromise)

e. Inappropriate computer use (Personnel do not remove CAC when leaving terminal, opening emails or attachments from suspicious or unknown entities).

f. Spillage or compromise via Social Media (Personal or Official).

g. Un-cleared workers or visitors in restricted areas without prior sanitization.

h. Theft / Loss of Government property (Radios, Laptops, Data, etc.).

i. Insider Threats.

j. Problematic organizational responses to OPSEC vulnerabilities (How an organization responds to known OPSEC violations, spillages, or compromises).

SECTION 2 – CRITICAL INFORMATION AND OPSEC MEASURES
2-3 AT/OPSEC COVERSHEET FOR CONTRACTS

1. The purpose of the AT/OPSEC Coversheet for contracts is to document the review of the requirements package statement of work statement (SOW), 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), Cybersecurity (CS), physical security (PS), law enforcement (LE), and foreign disclosure.

2. A signed AT/OPSEC cover sheet is required to be included in all requirements packages except for supply contracts under the simplified acquisition level threshold, field ordering officer actions and Government purchase card purchases.

3. The command / organization OPSEC Officer and Antiterrorism Officer (ATO) must review each requirements package prior to submission to the supporting contracting activity to include coordination with other staff elements for review as appropriate. If the requiring activity does not have an ATO or OPSEC Officer, the first ATO and OPSEC Officer in the chain of command will review the contract for considerations.

4. The most up to date AT/OPSEC Coversheet can be found in the USARJ Antiterrorism Teams folder at: https://armyeitaas.sharepoint-mil.us/:f:/r/teams/USARJG34Protection/Shared%20Documents/Antiterrorism/Admin?csf=1&web=1&e=q0Nac5

SECTION 2 – CRITICAL INFORMATION AND OPSEC MEASURES
2-4 USARJ SHRED POLICY

SUBJECT: USARJ Policy on Shredding of ALL Printed Materials

1. References:

   a. AR 25-55, Department of the Army Freedom of Information Act Program

   b. AR 380-5, Department of the Army Information Security Program

2. Purpose. To establish policy, procedure, and guidance on the disposal of materials containing PII and Sensitive but Unclassified Information.

3. When disposing of printed material that includes information from the USARJ Critical Information List or information that is otherwise critical, sensitive or Personal Identifiable Information (PII), USARJ personnel will shred the material by using a General Services Administration (GSA) approved shredder. This includes all printed documents and other media with information that is critical to military operations and personnel security, that are no longer needed to support USARJ administrative or operational requirements. The intent of this policy is to reduce the possibility of accidently disclosing critical or sensitive information.

4. The standards for destroying Controlled Unclassified Information (CUI) to include material previously labeled, For Official Use Only (FOUO), information and ensuring that critical and sensitive information generated or merely used by USARJ is properly destroyed is shredding. Shredding meets the requirement for destroying all classifications of printed material. Shredding is the most effective and practical means of destroying material in a way that prevents the possibility of it being reassembled. Shredding PII, critical and sensitive material therefore supports OPSEC. All printed materials that are classified PII, CUI, legacy FOUO or higher must be shredded.

5. OPSEC Officers will conduct periodic inspections of work areas, trash handling procedures, shared single point printing machines and areas, and recycling efforts throughout USARJ to monitor compliance with this policy.

6. The point of contact is the USARJ OPSEC Program Manager.

SECTION 3 – OPSEC RISK ASSESSMENT

3-1 OPSEC RISK ASSESSMENT PROCESS

1. The OPSEC analysis methodology uses a five step OPSEC Risk Assessment process. The basic risk analysis process allows an OPSEC manager to plan an effective OPSEC risk management strategy by analyzing and organizing information within each step of the process. An effective analysis is derived from using a basic calculation formula to establish specific risk levels relative to vulnerabilities based on the impact of the loss of the information, the threat posed to the information, and the susceptibility of the information to collection phases, each applied in sequential order.

USARJ OPSEC vulnerabilities:

a. STEP I. ASSIGN VALUE TO CRITICAL INFORMATION: Determine which items should reside on the unit/organization's Critical Information List (CIL).

(1) Step 1 establishes the value of critical information based on its importance to both adversary and friendly objectives and establishes subsequent impact to the organization or mission if that information is lost. Break down the CIL across specific Mission Areas and appropriate Subsets.

(2) Assign numeric values of 1 - 5 using weighted ranking to each element in each Mission Area. These values are consistent with the qualitative levels of assessment cited in DoDM 5205.02-M, (i.e. 1=LOW; 2=MED LOW; 3=MED; 4=MED HI; 5=HI).

(3) You will assign numeric value to the Assessed Value of the Critical Information to both Friendlies and Adversaries.

(4) You will total the numeric Assessed Value of the Critical Information to both Friendlies and Adversaries. *(See Section 3-2: Critical Value Matrix Worksheet)*

b. STEP II. PERFORM THREAT ANALYSIS**:**

(1) Determine what poses a threat to your organization by conducting a Threat Analysis. This process draws information from the most current All Hazards Threat Assessment (AHTA) and Counter-intelligence Assessments. Once you have identified adversaries who seek to gain a military, political, diplomatic, economic, or technological advantage you must assign threat values for each adversary across six Threat Vectors. These Threat Vectors include, HUMINT, SIGINT, OSINT, GEOINT, and MASINT.

(2) While assigning Threat Value you consider an adversary's assessed capability to collect information and their assessed intent. These values should be grounded in the information gathered and assess as part of your threat analysis.

(3) Assign numeric values of 1 - 5 using weighted ranking to adversary's assessed capability to collect information and their assessed intent. These values are consistent with the qualitative levels of assessment cited in the DoDM 5205.02-M, (i.e. 1=LOW; 2=MED LOW; 3=MED; 4=MED HI; 5=HI).

(4) The numeric value for threat is determined by multiplying the value assessed for Intent times the value assessed for Capability, (threat = intent x capability). Although we could cite other elements, (e.g. Opportunity, Targeting, History, etc.), this OPSEC Risk Analysis model cites Intent and Capability to be consistent with DoDM 5205.02-M. *(See Section 3-3: Threat Value Matrix Worksheet)*

c. STEP III. PERFORM VULNERABILITY ANALYSIS:

(1) Using the Mission Areas from the CIL, assess vulnerabilities of each Mission Area <u>subset</u> to adversarial collection from each of the five adversarial collection vectors, (e.g. HUMINT, SIGINT, OSINT, MASINT, GEOINT).

(2) Assign numeric values of 1 to 5 to each specific Mission Area item as they appear vulnerable to adversary collection by the six collection vectors.

(3) Only the highest vulnerability value to the overall MISSION AREA will be cited in the Risk Assessment Matrix Worksheet. *(See Section 3-4: Vulnerability Value Matrix Worksheet)*

d. STEP IV. PERFORM RISK ASSESSMENT:

(1) To achieve a quantitative value for assessing the risk of adversarial collection of critical information, a combination of previously completed assessment factors are blended and tallied in the risk assessment phase of this process. The Risk Assessment Matrix Worksheet contains Unit/Organization Critical Information divided into functional, Mission Areas. Each subset of each Mission Area contains a numeric value depicting its value/importance to the Unit/Organization.

(2) Using the data from the Critical Information Matrix Worksheet, enter the value for the Mission Area subset in the columns for each of the threat vectors. This value remains constant when factored against each adversarial threat collection vector because we value the item regardless of the threat.

(3) Using the data from the Threat Value Matrix Worksheet, enter the value of the assessed threat from each of the five threat vectors.

(4) Using the data from the Vulnerability Matrix Worksheet, enter the value of the assessed vulnerability to adversarial collection.

(5) The RISK SCORE is the sum of the Critical Information value, times the threat value, times the vulnerability value. (Risk = CI x Threat x Vulnerability. *(See Section 3-5: Risk Assessment Matrix Worksheet)*

(6) To assess the Commander's Overall Level of OPSEC Risk combine the totals for each Threat Vector across all Adversaries.

e. STEP V. IDENTIFY AND APPLY OPSEC MEASURES:

(1) OPEC Measures, [*including Action Control Measures, Countermeasures, and Counteranalysis*], are designed to prevent an adversary from detecting critical information, provide an alternative interpretation of critical information or indicators (deception), or deny the adversary's collection system. If the amount of risk is determined to be unacceptable, countermeasures are then implemented to mitigate risk or to establish an acceptable level. Countermeasures should be coordinated and integrated with other Information Operations core capabilities if applicable.

(2) There are many best practices for countermeasures throughout the DoD. Organizations may consult with OPSEC practitioners, security specialists, Cybersecurity, and organizations with similar missions. However, countermeasures should not be regarded as risk-avoidance measures to be pulled from a list and implemented.

(3) Examples of OPSEC Measures in which USARJ may employ:

(a) Action Control Measures are internal actions to eliminate the unit's unique indicators or vulnerabilities. Examples of Action Control Measures include:

1. Using secure communication equipment such as STU-III, STE, S-VOIP, etc.

2. Applying appropriate markings to information destined for dissemination.

3. Trash control (e.g. 100% shred policy)

4. Disseminating the unit Critical Information List (CIL) to all members of the unit.

5. Performing OPSEC training and briefings.

(b) OPSEC Countermeasures are designed to disrupt effective adversary collection. Examples of OPSEC Countermeasures include:

1. Electronic jamming (*counters SIGINT collection*).

2. Leveraging police: powers-of-arrest (*counters HUMINT collection*).

3. Coordinating activities with Counterintelligence assets (*counters HUMINT collection*).

(c) OPSEC Counteranalysis prevents accurate interpretations of what an adversary is able to see/observe about the unit. Examples of OPSEC Counteranalysis Measures include:

1. Deceptions and ruses.

2. Cover and Camouflage.

3. Use of decoys.

4. Truth projections through press/news releases.

2. Commands required to conduct an annual OPSEC risk assessment may use the five step OPSEC Risk Assessment process as outlined above or may use the OPSEC Risk module within DoD's Enterprise Risk Management System (EPRM) found on SIPR. For information regarding EPRM access and use contact the USARJ OPSEC OPR.

SECTION 3 – OPSEC RISK ASSESSMENT
3-2 OPSEC CRITICAL INFORMATION VALUE WORKSHEET

This step in the OPSEC Assessment process establishes the value of critical information based on its importance to both adversary and friendly objectives, and establishes subsequent impact to the organization or mission if that information is lost.

MISSION AREA / SUBSET	**CI ASSESSED VALUE**	
	FRIENDLY	**ADVERSARY**
MISSION AREA:		
Subset 1.		
Subset 2.		
etc.		
MISSION AREA:		
Subset 1.		
Subset 2.		
etc.		
MISSION AREA:		
Subset 1.		
Subset 2.		
etc.		
TOTALS		

CRITICAL INFORMATION VALUE DEFINITION TO UNIT	**WEIGHTED RANKING**	**CRITICAL INFORMATION VALUE DEFINITION TO ADVERSARY**	**WEIGHTED RANKING**
HIGH: Loss of critical information (CI) will have a SEVERE impact on our ability to accomplish the mission.	**5**	**HIGH:** This CI is of CRITICAL importance to an adversary and obtaining the information CONSIDERABLY contributes to meeting adversary objectives.	**5**
MEDIUM HIGH: Loss of CI will probably have a SERIOUS impact on our ability to accomplish the mission.	**4**	**MEDIUM HIGH:** This CI is of CRUCIAL importance to an adversary that obtaining the information APPRECIABLY contributes to meeting adversary objectives.	**4**
MEDIUM: Loss of CI will likely have an APPRECIABLE impact on our ability to accomplish the mission.	**3**	**MEDIUM:** This CI is of ESSENTIAL importance to an adversary that obtaining the information GREATLY contributes to meeting adversary objectives.	**3**
MEDIUM LOW: Loss of CI will possibly have a MODERATE impact on our ability to accomplish the mission.	**2**	**MEDIUM LOW:** This CI is of MODERATE importance to an adversary that obtaining the information contributes to meeting adversary objectives.	**2**
LOW: Loss of CI could have a MINOR impact on our ability to accomplish the mission.	**1**	**LOW:** This CI is MINOR importance to an adversary.	**1**

EXAMPLE

MISSION AREA / SUBSET	CI ASSESSED VALUE FRIENDLY	 ADVERSARY
MISSION AREA: COMMAND		
Subset 1. Mission times	5	5
Subset 2. Security Procedures	4	5
Subset 3. Aircrew home addresses	2	1
MISSION AREA: READINESS		
Subset 1. Supply and logistics levels	5	5
Subset 2. Budget information	3	2
MISSION AREA: COMMUNICATIONS		
Subset 1. IT infrastructure	5	4
Subset 2. Network diagrams	5	4
TOTALS	**29/35**	**26/35**

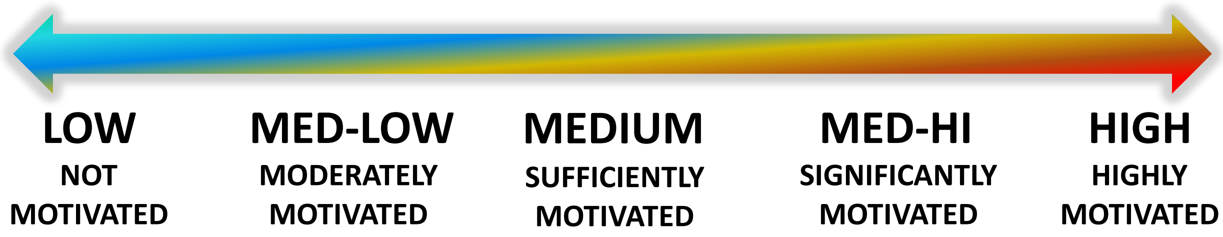
CIL ASSESSED VALUES RANKING SCALE	
THREAT	***VALUE***
HIGH	29-35
MED-HI	22-28
MEDIUM	15-21
MED-LOW	8-14
LOW	1-7

SECTION 3 – OPSEC RISK ASSESSMENT
3-3 OPSEC THREAT VALUE WORKSHEET

The threat assessment (TA) phase in the OPSEC process includes identifying potential adversaries in the operational environment and their associated capabilities, limitations, and intentions to collect, analyze, and use knowledge of our critical information against us. These ratings inform the Commander of the threat value to his critical information. You will use these values when performing the Risk Analysis phase of the OPSEC process.

		ASSESSED CAPABILITY to COLLECT				
	ADVERSARY: ***Threat Vector:***	5 HIGH	4 MED-HIGH	3 MED	2 MED-LOW	1 LOW
ASSESSED INTENT to COLLECT	5 - HIGH					
	4 - MED-HIGH					
	3 - MED					
	2 - MED-LOW					
	1 - LOW					

CAPABILITY VALUE DEFINITIONS:	**INTENT VALUE DEFINITIONS:**
5 - HIGH: The adversary's collection is highly developed and MOST LIKELY in place OR the adversary receives equivalent data collection support from a HIGHLY capable 3rd party.	**5 - HIGH:** The adversary is HIGHLY motivated and a successful outcome SIGNIFICANTLY contributes to meeting adversary objectives.
4 - MEDIUM-HIGH (MED HIGH): The adversary's collection capability is significantly developed and PROBABLY in place OR the adversary receives equivalent data collection support from a SIGNIFICANTLY capable 3rd party.	**4 - MEDIUM-HIGH (MED HIGH):** The adversary is SIGNIFICANTLY motivated and a successful outcome GREATLY contributes to meeting adversary objectives.
3 - MEDIUM: The adversary's collection capability is possibly developed and LIKELY in place OR the adversary receives equivalent data collection support from a CAPABLE 3rd party.	**3 - MEDIUM:** The adversary is SUFFICIENTLY motivated and a successful outcome WILL contribute to meeting adversary objectives.
2 - MEDIUM-LOW (MED LOW): The adversary's collection capability is probably not developed and MOST LIKELY NOT in place OR the adversary may receive equivalent data collection from a 3rd party.	**2 - MEDIUM-LOW (MED LOW):** The adversary is MODERATELY motivated and a successful outcome CAN contribute to meeting adversary objectives.
1 - LOW: The adversary collection capability is NOT developed OR does NOT receive data support from a 3rd party.	**1 - LOW**: The adversary is NOT motivated to collect information.



LOW NOT MOTIVATED

MED-LOW MODERATELY MOTIVATED

MEDIUM SUFFICIENTLY MOTIVATED

MED-HI SIGNIFICANTLY MOTIVATED

HIGH HIGHLY MOTIVATED

TERM	MEANING
INTENT to Collect	Assessment of the adversary's intentions to collect, analyze, and use knowledge of our critical information against us. This assessment is based upon intelligence and all-source reporting, history, current events, political-military relations with the U.S., Allies, and adversaries, and knowledge of the adversary's technical and non-technical collection abilities.
CAPABILITY to Collect	Assessment of the adversary's ability to collect our critical information. Includes technical and non-technical means of collection. This assessment is based upon intelligence and all-source reporting, history, and knowledge of the adversary's technical and non-technical collection abilities. Typical OPSEC assessments include the following intelligence and information collection vectors: CYBER (CNA/CNE), GEOINT, HUMINT, MASINT, OSINT, SIGINT.
LIKLIHOOD	The probability of an event or situation taking place.
NOT	Opportunities may exist however; there are no indications of interest, collection capability, or intent.
MODERATELY	Opportunities may exist. Adversary likely has interest but limited capability. No indications of intent or collection activity are present.
SUFFICIENTLY	Opportunities exist. Adversary has interest and collection capability. No indications of intent.
SIGNIFICANTLY	Opportunities exist. Adversary has interest and capability. Intent is present although no indications of specific current collection activity are underway.
HIGHLY	Opportunities exist. Adversary has interest and capability. Strong indications of intent. Confirmed indications of specific collection activity are underway.
CAN	Adversary is capable and opportunities exist. No indications of intent.
WILL	Adversary is capable, opportunities exist, and strong indications of intent are evident. Collection activity is either underway or imminent.

EXAMPLE

	ASSESSED CAPABILITY to COLLECT					
	ADVERSARY *(Fictional Republic)* ***Threat TYPE: HUMINT***	5 HIGH	4 MED-HIGH	3 MED	2 MED-LOW	1 LOW
ASSESSED INTENT to COLLECT	5 - HIGH					
	4 - MED-HIGH			12		
	3 - MED					
	2 - MED-LOW					
	1 - LOW					

4 (Intent) x 3 (capability) = 12

	ASSESSED CAPABILITY to COLLECT					
	ADVERSARY *(Fictional Republic)* ***Threat TYPE: SIGINT***	5 HIGH	4 MED-HIGH	3 MED	2 MED-LOW	1 LOW
ASSESSED INTENT to COLLECT	5 - HIGH					
	4 - MED-HIGH					
	3 - MED					
	2 - MED-LOW		8			
	1 - LOW					

2 (Intent) x 4 (Capability) = 8

	ASSESSED CAPABILITY to COLLECT					
	ADVERSARY *(Fictional Republic)* ***Threat TYPE: GEOINT***	5 HIGH	4 MED-HIGH	3 MED	2 MED-LOW	1 LOW
ASSESSED INTENT to COLLECT	5 - HIGH				10	
	4 - MED-HIGH					
	3 - MED					
	2 - MED-LOW					
	1 - LOW					

5 (Intent) x 2 (Capability) = 10

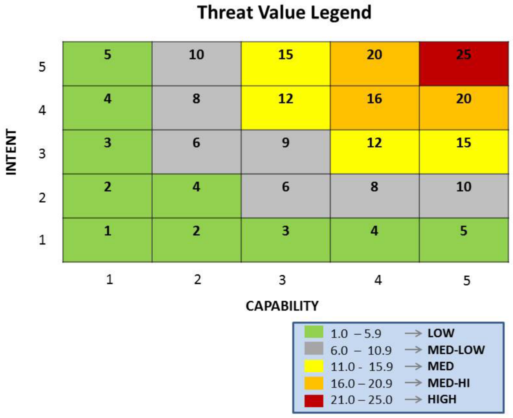
	ASSESSED CAPABILITY to COLLECT					
	ADVERSARY *(Fictional Republic)* ***Threat TYPE: OSINT***	5 HIGH	4 MED-HIGH	3 MED	2 MED-LOW	1 LOW
ASSESSED INTENT to COLLECT	5 - HIGH	25				
	4 - MED-HIGH					
	3 - MED					
	2 - MED-LOW					
	1 - LOW					

5 (Intent) x 5 (Capability) = 25

EXAMPLE

		ASSESSED CAPABILITY to COLLECT				
	ADVERSARY *(Fictional Republic)* ***Threat TYPE: MASINT***	5 HIGH	4 MED-HIGH	3 MED	2 MED-LOW	1 LOW
ASSESSED INTENT to COLLECT	5 - HIGH					
	4 - MED-HIGH					
	3 - MED					
	2 - MED-LOW					
	1 - LOW					1

1 (Intent) x 1 (Capability) = 1



Threat Value Legend

INTENT					
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
CAPABILITY	1	2	3	4	5

🟩	1.0 – 5.9	→ LOW
▨	6.0 – 10.9	→ MED-LOW
🟨	11.0 - 15.9	→ MED
🟧	16.0 – 20.9	→ MED-HI
🟥	21.0 – 25.0	→ HIGH

SUMMARY: (EXAMPLE)

Threat Assessment Table:

THREAT VECTOR	INTENT	CAPABILITY	SCORE
HUMINT	MED-HI	MED	12
SIGINT	MED-HI	MED-LOW	8
GEOINT	HIGH	MED-LOW	10
OSINT	HIGH	HIGH	25
MASINT	LOW	LOW	1
OVERALL THREAT VALUE:			**56** **MEDIUM**

OVERALL THREAT VALUE RANKING SCALE	
THREAT	***VALUE***
HIGH	121-150
MED-HI	91-120
MEDIUM	61-90
MED-LOW	31-60
LOW	1-30

SECTION 3 – OPSEC RISK ASSESSMENT
3-4 OPSEC VULNERABILITY VALUE WORKSHEET

The vulnerability assessment (VA) phase in the OPSEC process measures susceptibility of critical information to adversary collection. This step includes the identification of indicators that can also induce a susceptibility to adversary collection. These ratings inform the Commander of the vulnerability value of losing his critical information to adversarial collection. You will use these values when performing the Risk Analysis phase of the OPSEC process.

MISSION AREAS	**ASSESSED VULNERABILITY TO COLLECTION FROM ADVERSARY**						
		COLLECTION VECTOR					
		HUMINT	SIGINT	OSINT	MASINT	GEOINT	
	MISSION AREA:						
	Subset 1.						
	Subset 2.						
	etc.						
	MISSION AREA:						
	Subset 1.						
	Subset 2.						
	etc.						
	MISSION AREA:						
	Subset 1.						
	Subset 2.						
	etc.						

VULNERABILITY VALUE DEFINITIONS:
5 - HIGH: Exploitation of this vulnerability by an adversary will make critical information susceptible to at least one intelligence collection discipline virtually any time the adversary chooses to collect.
4 - MEDIUM-HIGH (MED HIGH): Exploitation of this vulnerability by an adversary will make critical information susceptible to at least one intelligence collection discipline most of the time the adversary chooses to collect.
3 - MEDIUM (MED): The adversary's capability to exploit this vulnerability is not well developed but could frequently make critical information susceptible to at least one intelligence collection discipline.
2 - MEDIUM-LOW (MED LOW): The adversary’s capability to exploit this vulnerability is poorly developed, and critical information is only occasionally susceptible to at least one intelligence collection discipline.
1 - LOW: Potential for exploitation is negligible.

EXAMPLE

MISSION AREAS	ASSESSED VULNERABILITY TO COLLECTION FROM ADVERSARY						
		COLLECTION VECTOR					
		HUMINT	SIGINT	OSINT	MASINT	GEOINT	
	MISSION AREA: COMMAND						
	Personnel rosters	3	1	2	1	1	
	Command priorities	3	1	2	1	1	
	MISSION AREA: READINESS						
	Training schedules	3	1	2	1	1	
	Training rosters	3	1	2	1	1	
	MISSION AREA: COMMS						
	Networks	1	5	1	1	3	
	Infrastructure	1	1	1	1	2	
	MISSION AREA: MOBILIZATION						
	Staging areas	3	3	3	3	5	
	Ports of Departure	3	3	2	1	5	
	TOTALS:	20	16	15	10	19	

Total possible value per column: 40

VULNERABILITY RANKING GUIDE *(BY INDIVIDUAL COLUMN)*	
HIGH	31-40
MED-HI	25-31
MEDIUM	17-24
MED-LOW	9-16
LOW	1-8

Vulnerability Rating (*in this example only*):

THREAT VECTOR	VALUE	VULNERABILITY RATING
HUMINT	20/40	MEDIUM
SIGINT	16/40	MED-LOW
OSINT	15/40	MED-LOW
MASINT	10/40	MED-LOW
GEOINT	19/40	MEDIUM
CYBER	26/40	MED-HI

SUMMARY: (EXAMPLE)

Vulnerability Assessment Table:

THREAT VECTOR	SCORE
HUMINT	20
SIGINT	16
GEOINT	10
OSINT	19
MASINT	26
OVERALL THREAT VALUE:	**91 MEDIUM-LOW**

OVERALL THREAT VALUE RANKING SCALE	
THREAT	***VALUE***
HIGH	193-240
MED-HI	145-192
MEDIUM	97-144
MED-LOW	49-96
LOW	1-48

SECTION 3 – OPSEC RISK ASSESSMENT
3-5 OPSEC RISK ASSESSMENT VALUE WORKSHEET

1. The risk assessment phase of the OPSEC process combines the findings and analysis of threats and vulnerabilities and is expressed as a measure of the probability that an adversary will be successful in collecting critical information and the resulting cost(s) to the mission.

2. Probability is determined by **multiplying** a vulnerability value by the relative threat value. This worksheet contains the matrices for determining probability and impact based on specific threat vector, (e.g. HUMINT, SIGINT, etc.), against identified vulnerabilities. It also contains a risk matrix worksheet for the combined risk value based upon all determined threats against all identified vulnerabilities.

3. To achieve a quantitative value for assessing the risk of adversarial collection of critical information, a combination of previously completed assessment factors are blended and tallied in the risk assessment phase of the OPSEC process. The Risk Assessment Matrix Worksheet contains Unit/Organization Critical Information divided into functional, Mission Areas. Each subset of each Mission Area contains a numeric value depicting its value/importance to the Unit/Organization.

a. Using the data from the Critical Information Matrix Worksheet, enter the value for the Mission Area subset in the columns for each of the threat vectors. This value remains constant when factored against each adversarial threat collection vector because we value the item regardless of the threat.

b. Using the data from the Threat Value Matrix Worksheet, enter the value of the assessed threat from each of the five (5) threat vectors.

c. Using the data from the Vulnerability Matrix Worksheet, enter the value of the assessed vulnerability to adversarial collection.

d. The RISK SCORE is the sum of the Critical Information value, times the threat value, times the vulnerability value. (Risk = CI x Threat x Vulnerability)

MISSION AREA:	**THREAT VECTOR**					
	HUMINT	**SIGINT**	**OSINT**	**MASINT**	**GEOINT**	
Subset 1.						
Threat						
Vulnerability						
RISK SCORE						
Subset 2.						
Threat						
Vulnerability						
RISK SCORE						
Subset 3.						
Threat						
Vulnerability						
RISK SCORE						

TOTAL RISK						

RISK VALUE		
🟥	501-625	HIGH
🟧	376-500	MED-HI
🟨	251-375	MEDIUM
▨	126-250	MED-LOW
🟩	0-125	LOW

TOTAL OVERALL RISK	
HIGH	12001-15000
MED-HI	9001-12000
MEDIUM	6001-9000
MED-LOW	3001-6000
LOW	0-3000

SECTION 3 – OPSEC RISK ASSESSMENT
3-6 OPSEC RISK ASSESSMENT PROCESS EXAMPLE

EXAMPLE

ADVERSARY BEING ASSESSED

1. **Insider Threat**

COLLECTION METHODS

1. Human Intelligence (HUMINT)
2. Signals Intelligence (SIGINT)
3. Open Source Intelligence (OSINT)
4. Measurement and Signature Intelligence (MASINT)
5. Geospatial Intelligence (GEOINT)
6. CYBER

VULNERABILITIES

1. Lack of understanding of OPSEC
2. Complacency in OPSEC policy enforcement
3. Discussion of sensitive information in unsecured / open areas
4. Throwing Sensitive / FOUO / PII in the trash
5. Inappropriate Computer use / Lack of Security (CAC removal / E-Mail)
6. Social Media (Personal / Official)
7. Schedules / Transportation Plans / Briefs
8. Contractor Workers / Visitors
9. Theft / Loss of Government property (Radios / Laptops / Data)

MEASURES

1. OPSEC Education & Training (Including Social Media Education & Training)
2. Positive control and accountability of Government Equipment
3. OPSEC disclosures in Contracts
4. Limit information (Need to know)
5. 100% shred policy
6. Properly Secure Information based on classification level
7. Encrypt email
8. Do not use DoD ID for other than military purposes
9. Enable screen lock on official cell phones

STEP 1: CRITICAL INFORMATION VALUE (INSIDER THREAT) WORKSHEET
EXAMPLE

MISSION AREA / SUBSET	CI ASSESSED VALUE	
	FRIENDLY	ADVERSARY
MISSION AREA: COMMAND		
Subset 1. Mission times	5	5
Subset 2. Security Procedures	4	5
Subset 3. Home addresses	2	4
MISSION AREA: READINESS		
Subset 1. Supply & Logistics	5	5
Subset 2. Budget Information	3	2
MISSION AREA: COMMUNICATIONS		
Subset 1. IT infrastructure	5	4
Subset 2. Network diagrams	5	4
TOTALS	**29/35**	**29/35**

QUANTITATIVE VALUE:

LOW:	1
MED-LOW:	2
MEDIUM:	3
MED-HIGH:	4
HIGH:	5

Total Value Possible:
NUMBER OF MISSION AREA SUBSET LINES X 5 = TOTAL VALUE POSSIBLE

OVERALL Assessed Friendly CI Value: 35

OVERALL Assessed Adversary CI Value: 35

STEP 2: CRITICAL THREAT VALUE (INSIDER THREAT) WORKSHEET

EXAMPLE

	ASSESSED CAPABILITY to COLLECT					
	ADVERSARY: Insider Threat ***Threat TYPE: HUMINT***	5 HIGH	4 MED-HIGH	3 MED	2 MED-LOW	1 LOW
ASSESSED INTENT to COLLECT	5 - HIGH	25				
	4 - MED-HIGH					
	3 - MED					
	2 - MED-LOW					
	1 - LOW					

5 (Intent) x 5 (capability) = 25

	ASSESSED CAPABILITY to COLLECT					
	ADVERSARY: Insider Threat ***Threat TYPE: SIGINT***	5 HIGH	4 MED-HIGH	3 MED	2 MED-LOW	1 LOW
ASSESSED INTENT to COLLECT	5 - HIGH					
	4 - MED-HIGH					
	3 - MED					
	2 - MED-LOW					
	1 - LOW					1

1 (Intent) x 1 (Capability) = 1

	ASSESSED CAPABILITY to COLLECT					
	ADVERSARY: Insider Threat ***Threat TYPE: GEOINT***	5 HIGH	4 MED-HIGH	3 MED	2 MED-LOW	1 LOW
ASSESSED INTENT to COLLECT	5 - HIGH					
	4 - MED-HIGH					
	3 - MED					
	2 - MED-LOW					
	1 - LOW					1

1 (Intent) x 1 (Capability) = 1

	ASSESSED CAPABILITY to COLLECT					
	ADVERSARY: Insider Threat ***Threat TYPE: OSINT***	5 HIGH	4 MED-HIGH	3 MED	2 MED-LOW	1 LOW
ASSESSE D INTENT to COLLECT	5 - HIGH	25				
	4 - MED-HIGH					
	3 - MED					
	2 - MED-LOW					
	1 - LOW					

5 (Intent) x 5 (Capability) = 25

EXAMPLE

	ASSESSED CAPABILITY to COLLECT					
	ADVERSARY: Insider Threat ***Threat TYPE: MASINT***	5 HIGH	4 MED-HIGH	3 MED	2 MED-LOW	1 LOW
ASSESSED INTENT to COLLECT	5 - HIGH					
	4 - MED-HIGH					
	3 - MED					
	2 - MED-LOW					
	1 - LOW					1

1 (Intent) x 1 (Capability) = 1

STEP 3: CRITICAL VULNERABILITY VALUE (INSIDER THREAT) WORKSHEET

EXAMPLE

MISSION AREAS	**ASSESSED VULNERABILITY TO COLLECTION FROM ADVERSARY**						
		COLLECTION VECTOR					
		HUMINT	SIGINT	OSINT	MASINT	GEOINT	
	MISSION AREA: COMMAND						
	Subset 1. Mission Times	5	1	2	1	1	
	Subset 2. Security Procedures	5	1	2	1	1	
	Subset 3. Home addresses	5	1	2	1	1	
	MISSION AREA: READINESS						
	Subset 1. Supply & Logistics	5	1	2	1	1	
	Subset 2. Budget information	5	1	2	1	1	
	MISSION AREA: COMMS						
	Subset 1. IT infrastructure	5	1	1	1	1	
	Subset 2. Network diagrams	5	1	1	1	1	
	TOTALS:	40	7	12	7	7	

Total possible value per column: 40

VULNERABILITY RANKING GUIDE *(BY INDIVIDUAL COLUMN)*	
HIGH	31-40
MED-HI	25-31
MEDIUM	17-24
MED-LOW	9-16
LOW	1-8

Vulnerability Rating (*in this example only*):

THREAT VECTOR	**VALUE**	**VULNERABILITY RATING**
HUMINT	40/40	HIGH
SIGINT	7/40	LOW
OSINT	12/40	MED-LOW
MASINT	7/40	LOW
GEOINT	7/40	LOW

SUMMARY: (EXAMPLE)

Vulnerability Assessment Table:

THREAT VECTOR	**SCORE**
HUMINT	40
SIGINT	7
GEOINT	7
OSINT	7
MASINT	21
OVERALL THREAT VALUE:	**82** **MED-LOW**

OVERALL THREAT VALUE RANKING SCALE	
THREAT	***VALUE***
HIGH	193-240
MED-HI	145-192
MEDIUM	97-144
MED-LOW	49-96
LOW	1-48

STEP 4: RISK ASSESSMENT (INSIDER THREAT) WORKSHEET

EXAMPLE

MISSION AREA: Command	**THREAT VECTOR**					
	HUMINT	**SIGINT**	**OSINT**	**MASINT**	**GEOINT**	
Subset 1. Mission Times	5	5	5	5	5	
Threat	25	1	25	1	1	
Vulnerability	5	1	2	1	1	
RISK SCORE	625	5	250	5	5	
Subset 2. Security Procedures	4	4	4	4	4	
Threat	25	1	25	1	1	
Vulnerability	5	1	2	1	1	
RISK SCORE	500	4	500	4	4	
Subset 3. Home Addresses	2	2	2	2	2	
Threat	25	1	25	1	1	
Vulnerability	5	1	2	1	1	
RISK SCORE	250	2	100	2	2	

EXAMPLE

MISSION AREA: Command	**THREAT VECTOR**					
	HUMINT	**SIGINT**	**OSINT**	**MASINT**	**GEOINT**	
Subset 1. Supply & Logistics	5	5	5	5	5	
Threat	25	1	25	1	1	
Vulnerability	5	1	2	1	1	
RISK SCORE	625	5	250	5	5	
Subset 2. Budget Information	3	3	3	3	3	
Threat	25	1	25	1	1	
Vulnerability	5	1	2	1	1	
RISK SCORE	375	3	150	3	3	

EXAMPLE

MISSION AREA: Communications	**THREAT VECTOR**					
	HUMINT	**SIGINT**	**OSINT**	**MASINT**	**GEOINT**	**CYBER**
Subset 1. IT Infrastructure	5	5	5	5	5	5
Threat	25	1	25	1	1	6
Vulnerability	5	1	1	1	1	3
RISK SCORE	625	5	125	5	5	90
Subset 2. Network Diagrams	5	5	5	5	5	5
Threat	25	1	25	1	1	6
Vulnerability	5	1	1	1	1	3
RISK SCORE	625	5	125	5	5	90

TOTAL RISK	3625	29	1500	29	29	522

Example Summary:
In this example HUMINT collection poses the most significant risk to the unit's Critical Information. This assessment would allow the OPSEC Program Manager to focus countermeasures and training efforts to mitigate the collection method and reduce the commander's overall level of acceptable risk.

SECTION 4 - REPORTS

4-1 OPSEC COMPROMISE REPORT

Commander's will submit an OPSEC compromise report when there is a confirmed disclosure of sensitive and/or critical information that jeopardizes a unit's ability to execute its mission or to adequately protect its personnel and/or equipment or negatively impacts national security. The OPSEC compromise report will be include the below information.

MEMORANDUM FOR RECORD

SUBJECT: OPSEC Compromise – Report of incidents concerning OPSEC

1. **OPSEC Compromise / Type of Incident** (i.e. but not limited to critical or sensitive information posted / released on open source; critical or sensitive information located in trash receptacle; unescorted visitor(s) in secured area; social engineering or attempts from unknown person(s) to gather sensitive information; phishing attempts; surveillance; social media; unauthorized cell phones or use of personal electronic devices in secured areas; badges worn in public area).

2. **Date / Time of Incident:**

3. **Location:**

4. **Personnel Involved:**

   Subject
   Name: (U//CUI)
   Rank:
   Position:
   Unit:
   Date of last known OPSEC training:

5. **Summary of Incident:** (CUI)

6. **Point of Contact:**

7: **Action Taken:** (OPSEC Measures taken i.e. but not limited to, removal of items of concern; retraining of person(s) involved; visitor control procedures; OPSEC reviews conducted; 100% shredding; use of encryption; use of lock-print; cell phone and PED policy).

SECTION 4 - REPORTS
4-2 INSIDER THREAT REPORTING

1. Commanders will ensure personnel are trained to identify potential risk indicators (PRI) of individuals at risk of becoming insider threats and report as required. PRI include a wide range of individual predispositions, stressors, choices, actions, and behaviors. Some indicators suggest increased vulnerability to insider threat; others may be signs of an imminent and serious threat.

2. Indicators do not always have diagnostic value or reflect wrongdoing and some PRI may involve activities that are constitutionally protected. Timely and appropriate reporting of PRI is crucial for assessing and mitigating insider threats. PRI will be reported in accordance with the USARJ Insider Threat Program.

3. Preventing harm due to insider threat is a shared responsibility and inherent to the USARJ OPSEC Program as unwitting insiders may inadvertently disclose sensitive information, cause spillage, unknowingly download malware, or facilitate cybersecurity events, causing damage to our national security.

4. The USARJ Insider Threat Program leverages other programs already in use in the command which will provide insight into useful approaches, transferable best practices, and techniques that can be tailored to prevent insider threats.

5. Insider Threat Program reporting requirements and processes are outlined in USARJ OPORD 23-08-009 (USARJ insider Threat Program).